HITRUST CSF PDF v11.2.0

THE HITRUST CSF INCLUDED IN THE DOWNLOAD PACKAGE IS NOT A COMPREHENSIVE LISTING OF ALL REQUIREMENTS WITHIN THE HITRUST CSF. THE FULL AND COMPREHENSIVE HITRUST CSF IS AVAILABLE ONLY UPON REQUEST TO ELIGIBLE QUALIFIED ORGANIZATIONS OR QUALIFIED INDIVIDUALS AS SET FORTH IN THE LICENSE AGREEMENT.

Qualified Organizations or Qualified Individuals may request access to the full and comprehensive HITRUST CSF PDF by submitting a request to info@hitrustalliance.net.

HITRUST will review requests to confirm the Qualified Organization or Qualified Individual eligibility. HITRUST reserves the right to reject any request, for the full and comprehensive HITRUST CSF, at HITRUST's sole discretion.

Table of Contents

Control Category: 0.0 - Information Security Management Program

Objective Name: 0.01 Information Security Management Program

Control Objective:	To implement and manage an Information Security Management Program.
Control Reference: 00.a Information Security Management Program	
Control Specification:	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust HITRUST De-ID Framework Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization has a formal information security management program (ISMP) that is documented and addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP is based on an accepted industry framework, considers all the control objectives of the accepted industry framework, documents any excluded control objectives of the accepted industry framework and the reasons for their exclusion, and is updated at least annually or when there are significant changes in the environment.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 23 NYCRR 500 - 500.03(g) Banking Requirements - FFIEC IS v2016 A.1.4 Banking Requirements - FFIEC IS v2016 A.2.2 Banking Requirements - FFIEC IS v2016 A.2.3 COBIT 5 APO13.02 COBIT 5 DS5.2 FTC Red Flags Rule (16 CFR 681) - 681.1e1 FTC Red Flags Rule (16 CFR 681) - 681.1e2 HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(iii) HITRUST De-ID Framework - De-ID Framework v1 Privacy and Security Program: General ISO/IEC 27001:2022 - 4.3a ISO/IEC 27001:2022 - 4.3d ISO/IEC 27001:2022 - 5.2b ISO/IEC 27001:2022 - 6.2f ISO/IEC 27001:2022 - 6.3 NIST SP 800-53 r5 - PL-10 NIST SP 800-53 r5 - PL-11 NY OHIP Moderate-Plus Security Baseline v5.0 - PL-11[IS.2] State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.210.2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 1
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust SCIDSA GDPR
Level 2 Implementation (example):	The information security management program (ISMP) has been established, implemented, operational, monitored, reviewed, and maintained. The ISMP is formally documented, protected, controlled, and retained according to federal, state and organizational requirements. The ISMP also incorporates a Plan, Do, Check, Act (PDCA) cycle for continuous improvement in the ISMP, particularly as information is obtained that could improve the ISMP, or indicates any shortcomings of the ISMP.

Level 2 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC3.1 Banking Requirements - FFIEC IS v2016 A.1.4 Banking Requirements - FFIEC IS v2016 A.2.2 Banking Requirements - FFIEC IS v2016 A.2.3 Banking Requirements - FFIEC IS v2016 A.2.8 Banking Requirements - FFIEC IS v2016 A.6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) ISO/IEC 27001:2022 - 4.4 ISO/IEC 27001:2022 - 5.1a ISO/IEC 27001:2022 - 5.1g ISO/IEC 27001:2022 - 5.2d ISO/IEC 27001:2022 - 6.1.1c ISO/IEC 27001:2022 - 6.1.1e2 ISO/IEC 27001:2022 - 7.5.3e NIST Cybersecurity Framework v1.1 - PR.IP-7 South Carolina Insurance Data Security Act (SCIDSA) - SCIDSA 33-99-20(G) The Joint Commission (v2016) - TJC IM.02.01.03, EP 1
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FISMA 23 NYCRR 500 Banking Requirements State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High)
Level 3 Implementation (example):	The information security management program (ISMP) has appropriate resources, roles, and responsibilities defined to establish, implement, operate, monitor, review, and maintain the ISMP. Further, independent audits also determine the continuing suitability, adequacy and effectiveness of the program. The organization continuously improves the ISMP through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventative actions and management review. The above requirements are to be formally defined and documented in the policies and/or standards.

Level 3 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC4.1 Banking Requirements - FFIEC IS v2016 A.1.4 Banking Requirements - FFIEC IS v2016 A.2.3 Banking Requirements - FFIEC IS v2016 A.2.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-13 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 HIPAA Security Rule - § 164.316(b)(1)(i) ISO/IEC 27001:2022 - 10.1 ISO/IEC 27001:2022 - 5.1b ISO/IEC 27001:2022 - 5.1c ISO/IEC 27001:2022 - 5.1e ISO/IEC 27001:2022 - 5.1f ISO/IEC 27001:2022 - 5.2c ISO/IEC 27001:2022 - 5.3a ISO/IEC 27001:2022 - 6.1.1a ISO/IEC 27001:2022 - 6.1.1b ISO/IEC 27001:2022 - 6.2e ISO/IEC 27001:2022 - 6.2g ISO/IEC 27001:2022 - 6.2h ISO/IEC 27001:2022 - 6.2i ISO/IEC 27001:2022 - 6.2j ISO/IEC 27001:2022 - 6.2k ISO/IEC 27001:2022 - 6.2l ISO/IEC 27001:2022 - 6.2m ISO/IEC 27001:2022 - 7.1 ISO/IEC 27001:2022 - 8.1b ISO/IEC 27001:2022 - 9.2.2e ISO/IEC 27001:2022 - 9.3.2d1 ISO/IEC 27001:2022 - 9.3.2d2 ISO/IEC 27001:2022 - 9.3.2d3 ISO/IEC 27001:2022 - 9.3.2f ISO/IEC 27001:2022 - 9.3.2g NIST Cybersecurity Framework v1.1 - PR.IP-7

Level CMS Implementation Requirements

Level CMS Implementation (example):	The organization develops and disseminates an organization-wide information security program plan that: provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. The organization: reviews the organization-wide information security program plan within every 365 days; updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and protects the information security program plan from unauthorized disclosure and modification.

	The organization: appoints a designated privacy official accountable for developing, implementing, and maintaining an organizational governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of Personally Identifiable Information (PII) by programs and information systems; monitors federal and state (as applicable) privacy laws and policies for changes that affect the privacy program; allocates appropriate budget and staffing resources to implement and operate the privacy program; develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and updates the privacy plan, policies, and procedures, as required, to address changing requirements, at least biannually.
Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	The organization determines if they are a hybrid organization as defined by HIPAA § 164.103 and if so, describe which parts of the organization are subject to HIPAA regulations and demonstrate how they are isolated from other portions of the business.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization develops, documents, and disseminates to organization-defined personnel or roles an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. The organization reviews and updates the current identification and authentication policy annually and identification and authentication procedures at least annually or whenever a significant change occurs. The organization develops, documents, and disseminates to organization-defined personnel or roles a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the security planning policy and associated security planning controls. The organization reviews and updates the current security planning policy annually, and security planning procedures at least annually or whenever a significant change occurs.
Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation (example):	Metrics are implemented by management that demonstrate the extent to which the information security management program is implemented and whether the program is effective. The metrics are timely, comprehensive, and actionable to improve the ISMP's effectiveness and efficiency.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization establishes, maintains, and resources an incident response plan for breaches involving personally identifiable information that contains an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms, and includes the identification of applicable privacy requirements. The organization ensures the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.

Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization provides sufficient information about the program management controls and common controls, including parameters for any assignment and selection statements of such controls either explicitly or by reference to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan, together, provide complete coverage for all security controls employed within the organization. The organization has a formal information security management program (ISMP) based on an accepted industry framework that is documented that addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP considers all the control objectives of the accepted industry framework and documents any excluded control objectives of the accepted industry framework and the reasons for their exclusion. The ISMP is updated at least annually or when there are significant changes in the environment. Further, the program plan is protected from unauthorized disclosure and modification.

Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation (example):	The organization is required to comply with Title 23 NYCRR Part 500 and has implemented a cybersecurity program that meets the requirements specified in Title 23 NYCRR Part 500, or adopted a cybersecurity program maintained by an affiliated entity, provided the program satisfies the requirements specified in NYCRR 500. All documentation and information relevant to the organization's cybersecurity program are made available to the financial services superintendent of New York upon request.

Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation (example):	Licensees have a formal information security program that, based on a risk assessment, is designed to mitigate identified risks, commensurate with the size, complexity, and sensitivity of the data which the licensee holds. The licensee designates a specific person, affiliate, or entity to be responsible for the program. Insurers are annually submitting a written statement by the 15th of February, certifying compliance with the South Carolina Data Security Act. Insurers maintain all required records for a period of five years.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization establishes, maintains, and resources a system and information integrity plan that includes: a continuous monitoring strategy and a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy. The organization develops a continuous monitoring strategy. The organization implements a continuous monitoring program that includes reporting the security status of the organization and information system to defined personnel or roles (defined in the applicable system security plan) monthly.

Level DGF Implementation Requirements	
Level DGF Implementation (example):	The organization has a formally defined Data Governance program with defined vision and goals. A consistent framework is used to manage Data Governance.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization establishes, maintains, and resources an access control plan that includes: a mission and/or vision statement; strategic goals/objectives, preferably in SMART format (i.e., Specific, Measurable, Attainable, Result-focused, Time-bound); a project plan to record activities, due dates, and organizational resources (e.g., funding, people, tools) assigned to the management or oversight of access control activities; training needed to perform the access control activities; involvement of relevant stakeholders; resources necessary to support all related activities; a defined frequency for plan review, typically no less than every 365 days; relevant standards and procedures with a focus on establishing system access requirements; relevant standards and procedures with a focus on controlling internal system access; relevant standards and procedures with a focus on controlling remote system access; and relevant standards and procedures with a focus on limiting data access to authorized users and processes. The organization establishes, maintains, and resources an identification and authentication plan that includes: a mission and/or vision statement; strategic goals/objectives, preferably in SMART format (i.e., Specific, Measurable, Attainable, Result-focused, Time-bound); a project plan to record activities, due dates, and organizational resources (e.g., funding, people, tools) assigned to the management or oversight of identification and authentication activities; training needed to perform the identification and authentication activities; involvement of relevant stakeholders; resources necessary to support all related activities; a defined frequency for plan review, typically no less than every 365 days; and relevant standards and procedures with a focus on granting access to authentication entities.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization establishes, maintains, and resources an awareness and training plan that includes: a mission and/or vision statement; strategic goals/objectives, preferably in SMART format (i.e., Specific, Measurable, Attainable, Result-focused, Time-bound); a project plan to record activities, due dates, and organizational resources (e.g., funding, people, tools) assigned to the management or oversight of awareness and training activities; training needed to perform the awareness and training activities; involvement of relevant stakeholders; resources necessary to support all related activities; a defined frequency for plan review, typically no less than every 365 days; relevant standards and procedures with a focus on conducting security awareness activities; and relevant standards and procedures with a focus on conducting training.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The organization manages individual identifiers by uniquely identifying each individual based on organization-defined characteristics, including contractor, foreign national, and non-organizational user.
Level ISO/IEC 27001 Implementation Requirements	
Level ISO/IEC 27001 Implementation (example):	The organization requires information security management documentation contain sufficient identification and description (e.g. a title, date, author, or reference number), and adhere to an appropriate format (e.g. language, software version, graphics) and media (e.g. paper, electronic).

Control Category: 01.0 - Access Control

Objective Name: 01.01 Business Requirement for Access Control

Control Objective:	To control access to information, information assets, and business processes based on business and security requirements.

Control Reference: 01.a Access Control Policy

Control Specification:	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA HITRUST De-ID Framework The Joint Commission v2016 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 1 Implementation (example):	Access control rules and rights for each user or group of users are based on clearly defined requirements for information dissemination and authorization (e.g., need-to-know, need-to-share, least privilege, security levels, and information classification). The policy further defines logical and physical access control rules and rights for each user or group of users are considered together and clearly defined in standard user access profiles (e.g., roles). The access control program takes into account security requirements of individual business applications and business units and ensures standard user access profiles for common jobs roles in the organization.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 21 CFR Part 11.10(d) 23 NYCRR 500 - 500.03(d) 23 NYCRR 500 - 500.12(a) AICPA Trust Services Criteria - AICPA 2017 CC5.2 AICPA Trust Services Criteria - AICPA 2017 CC6.1 AICPA Trust Services Criteria - AICPA 2017 CC6.3 AICPA Trust Services Criteria - AICPA 2017 CC6.4 AICPA Trust Services Criteria - AICPA 2017 CC6.8 Banking Requirements - FFIEC IS v2016 A.6.22(d) Banking Requirements - FFIEC IS v2016 A.6.8(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) FedRAMP - AC-6[H] FedRAMP - AC-6[M] Health Industry Cybersecurity Practices - 3.L.B Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.312(a)(1) HITRUST De-ID Framework - De-ID Framework v1 Access Control: General IRS Pub 1075 - AC-2c IRS Pub 1075 - AC-2d3 IRS Pub 1075 - AC-6 ISO/IEC 27002:2022 - 5(18) ISO/IEC 27002:2022 - 8(2) ISO/IEC 27002:2022 - 8(22) ISO/IEC 27799:2016 9.1.1 MARS-E v2.2 - AC-6 NIST Cybersecurity Framework v1.1 - PR.PT-3 NIST SP 800-171 r2 - 3.1.5[a] NIST SP 800-171 r2 - 3.1.5[b] NIST SP 800-171 r2 - 3.1.5[c] NIST SP 800-171 r2 - 3.1.5[d] NIST SP 800-171 r2 - 3.4.6[a] NIST SP 800-171 r2 - 3.4.6[b] NIST SP 800-53 R4 AC-6[HM]{0} NIST SP 800-53 R4 SA-17(7)[S]{0} NIST SP 800-53 r5 - AC-6 NIST SP 800-53 r5 - SA-17(7) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2d2 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2d3 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6[IS.4] Supplemental Requirements - SR v6.4 16-0 Supplemental Requirements - SR v6.4 41-1 Supplemental Requirements - SR v6.4 7b.1-2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 1 Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(a) Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(b) Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(g)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FISMA HITRUST De-ID Framework The Joint Commission v2016 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	The organization ensures users and service providers are given a clear statement of the business requirements to be met by access controls. The access control policy defines business requirements and how access controls are used to protect data. The access control policy defines requirements for formal authorization of access requests, modification of permissions/rights/access, emergency access, periodic review of access rights, and the removal of access. Further, the organization develops and disseminates/communicates a formal access control program (e.g., through policies and procedures) and reviews and updates the program annually.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC6.2 Banking Requirements - FFIEC IS v2016 A.6.22(d) Banking Requirements - FFIEC IS v2016 A.6.8(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(3)(i) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.312(a)(2)(ii) IRS Pub 1075 - AC-1c1 IRS Pub 1075 - AC-1c2 ISO/IEC 27002:2022 - 5(15) ISO/IEC 27002:2022 - 5(16) ISO/IEC 27799:2016 9.1.1 NIST SP 800-53 R4 AC-3(4)[S]{1} NIST SP 800-53 R4 AC-3(8)[S]{0} NIST SP 800-53 r5 - AC-3(4) NIST SP 800-53 r5 - AC-3(8) Supplemental Requirements - SR v6.4 19-0 The Joint Commission (v2016) - TJC IM.02.01.03, EP 1

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Banking Requirements
Level 3 Implementation (example):	Information related to the business applications and risks the information is facing is identified. Access control and information classification policies of different systems and networks are consistent. Access rights are managed for all types of connections available in a distributed and networked environment.
Level 3 Authoritative Source Mapping:	ISO/IEC 27799:2016 9.1.1 ISO/IEC 27799:2016 9.1.2 ISO/IEC 27799:2016 9.2.1 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 r5 - PS-3(3)a NIST SP 800-53 r5 - SC-50
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization enforces role-based access control policies over all subjects and objects uniformly within the boundary of the information system. The organization enforces role-based access control policies over all subjects and objects where the policy specifies that a subject that has been granted access to information is constrained from passing the information to unauthorized subjects or objects, granting its privileges to other subjects, changing one or more security attributes on subjects, objects, the information system, or information system components, and choosing the security attribute and attribute values to be associated with newly created or modified objects.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. The organization reviews and updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization develops, documents, and disseminates to applicable personnel an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

	The organization only permits the use of shared/group accounts when a business need can be documented and approved, in advance, by the Authorizing Official (AO). When shared/group accounts are used, the applicable System Security Plan (SSP) describes how the shared/group accounts are used and includes compensating processes and procedures implemented to provide the ability to uniquely attribute account user activities.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization develops, documents, and disseminates to organization-defined personnel or roles: an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the access control policy and associated access controls; and reviews and updates the current: access control policy and access control procedures within organization-defined frequency. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level access control policy that is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization uses access governance tools to prevent or detect segregation of incompatible duties conflicts across critical information systems, and to facilitate the periodic review of access rights.

Objective Name: 01.02 Authorized Access to Information Systems

Control Objective:	To ensure authorized user accounts are registered, tracked, and periodically validated to prevent unauthorized access to information systems.

Control Reference: 01.b User Registration

Control Specification:	There shall be a formal documented and implemented user registration and de-registration procedure for granting and revoking access.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	The Joint Commission v2016 CA Civil Code § 1798.81.5 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act
Level 1 Implementation (example):	Default and unnecessary accounts are removed, disabled, or otherwise secured.

Level 1 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.20(e) Banking Requirements - FFIEC IS v2016 A.6.27(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2[IS.1] PCI DSS v3.2.1 8.1.2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(a) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(d) Supplemental Requirements - SR v6.4 6.5-0 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No Is the system(s) accessible from the Internet? Yes Are hardware tokens used as an authentication method within the scoped environment? No
Level 2 Regulatory Factors:	DirectTrust The Joint Commission v2016 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate Supplemental
Level 2 Implementation (example):	Proper identification is required for requests to establish information system accounts and approval of requests to establish such accounts. Account managers are notified when users are: terminated, transferred, their information system usage or need-to-know/need-to-share changes, or when accounts (including shared/group, emergency, and temporary accounts) are no longer required. Account managers modify the user's account accordingly.

Level 2 Authoritative Source Mapping:	21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 21 CFR Part 11.100(b) AICPA Trust Services Criteria - AICPA 2017 CC5.2 AICPA Trust Services Criteria - AICPA 2017 CC6.2 AICPA Trust Services Criteria - AICPA 2017 CC6.3 Banking Requirements - FFIEC IS v2016 A.6.20(a) Banking Requirements - FFIEC IS v2016 A.6.20(b) CIS Controls v7.1 - CIS CSC v7.1 16.10 CIS Controls v7.1 - CIS CSC v7.1 16.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(03) (HIGH; MOD) COBIT 5 DS5.3 COBIT 5 DS5.4 COBIT 5 DSS05.03 COBIT 5 DSS05.04 EHNAC Accreditation Committee FedRAMP - AC-2(10)[H] FedRAMP - AC-2(10)[M] FedRAMP - AC-2c[H] FedRAMP - AC-2c[L] FedRAMP - AC-2c[M] FedRAMP - AC-2h1[H] FedRAMP - AC-2h1[L] FedRAMP - AC-2h1[M] FedRAMP - AC-2h2[H] FedRAMP - AC-2h2[L] FedRAMP - AC-2h2[M] FedRAMP - AC-2h3[H] FedRAMP - AC-2h3[L] FedRAMP - AC-2h3[M] FedRAMP - AC-2k[H] FedRAMP - AC-2k[L] FedRAMP - AC-2k[M] FedRAMP - IA-5(3)[H] FedRAMP - IA-5(3)[M] FedRAMP - PS-3(3)a[H] FedRAMP - PS-3(3)a[M] FedRAMP - PS-4f[H] FedRAMP - PS-4f[L] FedRAMP - PS-4f[M] Health Industry Cybersecurity Practices - 3.S.A HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.308(a)(5)(ii)(D) HIPAA Security Rule - § 164.312(a)(2)(ii) HIPAA Security Rule - § 164.312(d) IRS Pub 1075 - AC-2a IRS Pub 1075 - AC-2d2 IRS Pub 1075 - IA-12(1) IRS Pub 1075 - IA-12(2) IRS Pub 1075 - IA-12a ISO/IEC 27799:2016 9.2.1 ISO/IEC 27799:2016 9.2.2

Level 2 Authoritative Source Mapping (Cont.):	Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-2(10) MARS-E v2.2 - AC-2a MARS-E v2.2 - AC-2c MARS-E v2.2 - AC-2h1 MARS-E v2.2 - AC-2h2 MARS-E v2.2 - AC-2h3 MARS-E v2.2 - AC-2k MARS-E v2.2 - IA-5(3) NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST Cybersecurity Framework v1.1 - PR.AC-4 NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST SP 800-171 r2 - 3.5.2[a] NIST SP 800-171 r2 - 3.5.2[b] NIST SP 800-171 r2 - 3.5.2[c] NIST SP 800-53 R4 AC-2(10)[S]{0} NIST SP 800-53 R4 AC-2c[HML]{0} NIST SP 800-53 R4 AC-2d[HML]{0} NIST SP 800-53 R4 AC-2e[HML]{0} NIST SP 800-53 R4 AC-2f[HML]{0} NIST SP 800-53 R4 AC-2h[HML]{0} NIST SP 800-53 R4 AC-2i[HML]{3} NIST SP 800-53 R4 AC-2k[HML]{0} NIST SP 800-53 R4 IA-4(2)[S]{0} NIST SP 800-53 R4 IA-4(3)[S]{2} NIST SP 800-53 R4 IA-4(7)[S]{0} NIST SP 800-53 R4 IA-5(3)[HM]{0} NIST SP 800-53 R4 PS-3(3)a[S]{0} NIST SP 800-53 R4 PS-4f[HML]{0} NIST SP 800-53 R4 PS-5d[HML]{0} NIST SP 800-53 R4 PS-6(2)a[S]{0} NIST SP 800-53 R4 PS-6(2)b[S]{0} NIST SP 800-53 r5 - AC-2a NIST SP 800-53 r5 - AC-2c NIST SP 800-53 r5 - AC-2d1 NIST SP 800-53 r5 - AC-2d2 NIST SP 800-53 r5 - AC-2d3 NIST SP 800-53 r5 - AC-2e NIST SP 800-53 r5 - AC-2f NIST SP 800-53 r5 - AC-2h NIST SP 800-53 r5 - AC-2i3 NIST SP 800-53 r5 - AC-2k NIST SP 800-53 r5 - AC-2l NIST SP 800-53 r5 - IA-12 NIST SP 800-53 r5 - IA-12(2) NIST SP 800-53 r5 - IA-12(3) NIST SP 800-53 r5 - IA-12(4) NIST SP 800-53 r5 - PS-3(3)a NIST SP 800-53 r5 - PS-5d NIST SP 800-53 r5 - PS-6(2)a NIST SP 800-53 r5 - PS-6(2)b NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2(9)[NYS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2a NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2c NY OHIP Moderate-Plus Security Baseline v5.0 - CM-12b NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12(3) NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12(3)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12a

Level 2 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12c NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3[IS.4b] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3e2 NY OHIP Moderate-Plus Security Baseline v5.0 - SA-21a OCR Audit Protocol (2016) 164.308(a)(3)(ii)(A) PCI DSS v3.2.1 8.1.2 PCI DSS v3.2.1 8.1.3 PCI DSS v3.2.1 8.1.4 PCI DSS v3.2.1 8.5 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(d) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(a) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(b) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(d) Supplemental Requirements - SR v6.4 19a-0 Supplemental Requirements - SR v6.4 19c-0 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5 Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(g)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 3 Implementation (example):	Automated mechanisms support the management of information system accounts, including the disabling of emergency accounts within 24 hours, and temporary accounts within a fixed duration not to exceed 365 days. In addition to assigning a unique ID and password, token devices (e.g., SecurID, certificates, public key), biometrics, or both methods are employed to authenticate all users.
Level 3 Authoritative Source Mapping:	FedRAMP - AC-2(1)[H] FedRAMP - AC-2(1)[M] HIPAA Security Rule - § 164.312(a)(2)(i) IRS Pub 1075 - AC-2(1) NIST Cybersecurity Framework v1.1 - PR.AC-7 NIST SP 800-53 R4 AC-2(1)[HM]{0} NIST SP 800-53 R4 AC-2(2)[HM]{0} NIST SP 800-53 R4 AC-2(8)[S]{0} NIST SP 800-53 r5 - AC-2(1) NIST SP 800-53 r5 - AC-2(2) NIST SP 800-53 r5 - AC-2(8) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2(1) PCI DSS v3.2.1 8.2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Level CMS Implementation Requirements

Level CMS Implementation (example):	Automated mechanisms support the management of information system accounts, including the disabling of emergency accounts within 24 hours and temporary accounts within a fixed duration not to exceed 30 days.

	The organization disables accounts of users posing a significant risk immediately, not to exceed 30 minutes after discovery of the risk.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system automatically disables inactive accounts after 35 days for user accounts. Automated mechanisms support the management of information system accounts, including the disabling of emergency and temporary accounts within 24 hours.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization maintains a policy addressing issuance of appropriate authorization credentials, including badges, identification cards or smart cards. The organization notifies account managers and designated agency officials within 24 hours when accounts are no longer required.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system automatically disables inactive accounts within 60 days. The organization disables accounts of users posing a significant risk within 60 minutes of discovery of the risk.

Control Reference: 01.c Privilege Management

Control Specification:	The allocation and use of privileges to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 1 Regulatory Factors:	DirectTrust FedRAMP FISMA The Joint Commission v2016 CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 1 Implementation (example):	The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed). The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users and tracks and monitors privileged role assignments.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 23 NYCRR 500 - 500.07 AICPA Trust Services Criteria - AICPA 2017 CC6.2 AICPA Trust Services Criteria - AICPA 2017 CC6.3 AICPA Trust Services Criteria - AICPA 2017 CC6.8 Banking Requirements - FFIEC IS v2016 A.6.20(d) Banking Requirements - FFIEC IS v2016 A.6.21(a) Banking Requirements - FFIEC IS v2016 A.6.22(b) Banking Requirements - FFIEC IS v2016 A.6.29 Banking Requirements - FFIEC IS v2016 A.6.8(c) CIS Controls v7.1 - CIS CSC v7.1 4.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(03) (HIGH) COBIT 5 DS5.4 COBIT 5 DSS05.04 FedRAMP - AC-2(7)b[H] FedRAMP - AC-2(7)b[M] FedRAMP - AC-3[L] FedRAMP - AC-3[M] FedRAMP - AC-6(2)[H] FedRAMP - AC-6(2)[M] Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 3.S.A Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.312(a)(1) HITRUST De-ID Framework - De-ID Framework v1 Identification and Authentication (Application-level): Authentication Policy IRS Pub 1075 - AC-2(7)c IRS Pub 1075 - AC-6(2) IRS Pub 1075 - AC-6(IRS-1) IRS Pub 1075 - AC-6(IRS-2) ISO/IEC 27799:2016 9.2.3 MARS-E v2.2 - AC-2(7)c MARS-E v2.2 - AC-3 MARS-E v2.2 - AC-5a NIST SP 800-53 R4 AC-21(2)[S]{0} NIST SP 800-53 R4 AC-3[HML]{0} NIST SP 800-53 R4 AC-6(4)[S]{0} NIST SP 800-53 R4 CM-5(5)a[S]{1} NIST SP 800-53 r5 - AC-21(2) NIST SP 800-53 r5 - AC-2c NIST SP 800-53 r5 - AC-3 NIST SP 800-53 r5 - AC-6(4) NIST SP 800-53 r5 - CM-5(5)a NIST SP 800-53 r5 - IA-12(1) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-5[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(5) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-2(2)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3(3)a PCI DSS v3.2.1 7.1 PCI DSS v3.2.1 7.1.1

Level 1 Authoritative Source Mapping (Cont.):	PCI DSS v3.2.1 7.1.4 PCI DSS v3.2.1 7.2.1 PCI DSS v3.2.1 7.2.2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(a) Supplemental Requirements - SR v6.4 5-0 Supplemental Requirements - SR v6.4 7a.1-0 Supplemental Requirements - SR v6.4 7a.3-0 Supplemental Requirements - SR v6.4 7b.1-1 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5 Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(g)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of users of the system(s) 500 to 5,500 Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No
Level 2 Regulatory Factors:	HITRUST De-ID Framework Banking Requirements High Moderate
Level 2 Implementation (example):	Role-based access controls are implemented and capable of mapping each user to one or more roles, and each role to one or more system functions. The development and use of system routines and programs which avoid the need to run elevated privileges is promoted.

Level 2 Authoritative Source Mapping:	21 CFR Part 11.10(d) AICPA Trust Services Criteria - AICPA 2017 CC6.3 Banking Requirements - FFIEC IS v2016 A.6.20(d) Banking Requirements - FFIEC IS v2016 A.6.22(b) Banking Requirements - FFIEC IS v2016 A.6.27(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-10 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-21 (HIGH; MOD) FedRAMP - AC-6(5)[H] FedRAMP - AC-6(5)[M] Health Industry Cybersecurity Practices - 3.L.B Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 3.S.A HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.312(a)(1) HITRUST De-ID Framework - De-ID Framework v1 Access Control: Access Policies IRS Pub 1075 - AC-6(6) ISO/IEC 27002:2022 - 8(2) ISO/IEC 27799:2016 9.1.1 ISO/IEC 27799:2016 9.2.3 MARS-E v2.2 - AC-5a MARS-E v2.2 - AC-6(5) NIST Cybersecurity Framework v1.1 - PR.AC-4 NIST SP 800-171 r2 - 3.1.6[a] NIST SP 800-171 r2 - 3.1.6[b] NIST SP 800-53 R4 AC-21[HM]{0} NIST SP 800-53 R4 AC-6(5)[HM]{0} NIST SP 800-53 r5 - AC-21 NIST SP 800-53 r5 - AC-3(15)b NIST SP 800-53 r5 - AC-6(5) NIST SP 800-53 r5 - SA-8(14) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-17(4)a PCI DSS v3.2.1 7.1.2 PCI DSS v3.2.1 7.1.3 PCI DSS v3.2.1 7.2 PCI DSS v3.2.1 7.2.3 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500 Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No

Level 3 Regulatory Factors:	FedRAMP FISMA The Joint Commission v2016 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	The organization explicitly authorizes access to the following security functions (deployed in hardware, software, and firmware) and security-relevant information: Setting/modifying audit logs and auditing behavior; Setting/modifying boundary protection system rules; Configuring/modifying access authorizations (e.g., permissions, privileges); Setting/modifying authentication parameters; and Setting/modifying system configurations and parameters. The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions including disabling, circumventing, or altering implemented security safeguards (e.g., IDS/IPS or malicious code protection mechanisms).

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC6.8 Banking Requirements - FFIEC IS v2016 A.6.21(a) CIS Controls v7.1 - CIS CSC v7.1 14.6 CIS Controls v7.1 - CIS CSC v7.1 4.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(09) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(10) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) FedRAMP - AC-6(1)[H] FedRAMP - AC-6(1)[M] FedRAMP - AC-6(10)[H] FedRAMP - AC-6(10)[M] FedRAMP - AC-6(9)[H] FedRAMP - AC-6(9)[M] FedRAMP - PS-7b[H] FedRAMP - PS-7b[L] FedRAMP - PS-7b[M] HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(a)(2)(iii) IRS Pub 1075 - AC-6(1)a IRS Pub 1075 - AC-6(1)b IRS Pub 1075 - AC-6(10) IRS Pub 1075 - AC-6(9) IRS Pub 1075 - PS-7b Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-2a MARS-E v2.2 - AC-6 MARS-E v2.2 - AC-6(1)a MARS-E v2.2 - AC-6(1)b MARS-E v2.2 - AC-6(1)c MARS-E v2.2 - AC-6(1)d MARS-E v2.2 - AC-6(1)e MARS-E v2.2 - AC-6(10) MARS-E v2.2 - AC-6(9) MARS-E v2.2 - PS-7a NIST Cybersecurity Framework v1.1 - PR.IP-1 NIST Cybersecurity Framework v1.1 - PR.PT-3 NIST SP 800-171 r2 - 3.1.1[d] NIST SP 800-171 r2 - 3.1.1[e] NIST SP 800-171 r2 - 3.1.7[a] NIST SP 800-171 r2 - 3.1.7[b] NIST SP 800-171 r2 - 3.1.7[c] NIST SP 800-171 r2 - 3.1.7[d] NIST SP 800-53 R4 AC-3(10)[S]{0} NIST SP 800-53 R4 AC-3(3)[S]{4} NIST SP 800-53 R4 AC-6(1)[HM]{0} NIST SP 800-53 R4 AC-6(10)[HM]{0} NIST SP 800-53 R4 AC-6(6)[S]{0} NIST SP 800-53 R4 AC-6(8)[S]{0} NIST SP 800-53 R4 AC-6(9)[HM]{0} NIST SP 800-53 R4 AU-10[H]{2} NIST SP 800-53 R4 CM-5(5)a[S]{2} NIST SP 800-53 R4 PS-7b[HML]{0} NIST SP 800-53 R4 SC-3[H]{0} NIST SP 800-53 R4 SC-34(3)[S]{0}

Level 3 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - AC-3(10) NIST SP 800-53 r5 - AC-3(3) NIST SP 800-53 r5 - AC-6(1) NIST SP 800-53 r5 - AC-6(10) NIST SP 800-53 r5 - AC-6(6) NIST SP 800-53 r5 - AC-6(8) NIST SP 800-53 r5 - AC-6(9) NIST SP 800-53 r5 - AU-10 NIST SP 800-53 r5 - CM-5(5)a NIST SP 800-53 r5 - SA-8(14) NIST SP 800-53 r5 - SA-8(31) NIST SP 800-53 r5 - SC-3 NIST SP 800-53 r5 - SC-51 NIST SP 800-53 r5 - SI-7(10) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(1)b1 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(1)b2 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(1)b3 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(1)b4 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(1)b5 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(10) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-7[IS.1] PCI DSS v3.2.1 7.2.2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization uses automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. The organization validates that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive. Administrators use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine is isolated from the organization's primary network and is not allowed Internet access. This machine is not used for reading email, composing documents, or surfing the Internet.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	All system and removable media boot access is disabled unless it is explicitly authorized by the organizational CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected. The organization authorizes network access to privileged commands only for compelling operational needs as defined in the system security plan and documents the rationale for the information system.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	A role-based approach is used to establish and administer privileged user accounts, including application-specific privileged user accounts based on the responsibilities associated with the use of each application. Privileged roles are monitored, and actions are taken when privileged role assignments are no longer appropriate. The information system prevents any software except software explicitly documented from executing at higher privilege levels than users executing the software.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization restricts the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards. FTI received under U.S.C. Title 26 § 6103 is confidential and not disclosed, except as provided by U.S.C. Title 26 § 6103(a).
Level HIE Implementation Requirements	
Level HIE Implementation (example):	The organization, acting as a HIE, defines and assigns roles to all employees and to all employees of connecting organizations with access to the HIE. The roles are based on the individuals' job function and responsibilities. The roles specify the type of access and level of access.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	A role-based access approach is used to establish and administer privileged user accounts, including application-specific privileged user accounts based on the responsibilities associated with the use of each application. Privileged roles are monitored. The information system does not release information outside of the established system boundary unless the receiving organization provides appropriate security safeguards. The safeguards are used to validate the appropriateness of the information designated for release.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	A service provider protects each organization's hosted environment and data by: ensuring that each organization only runs processes that only have access to that organization's cardholder data environment, and restricting each organization's access and privileges to only its own cardholder data environment.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	Shared accounts must have strictly limited permissions and access only to the system(s) required. The organization restricts the use of database management utilities to only authorized database administrators, prevents users from accessing database data files at the logical data view, field, or field-value level, and implements table-level access control.
Level NIST SP 800-53 Implementation Requirements	

Control Reference: 01.d User Password Management

Control Specification:	Passwords shall be controlled through a formal management process.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	

Level 1 Regulatory Factors:	CA Civil Code § 1798.81.5 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Supplemental
Level 1 Implementation (example):	User identities are verified prior to performing password resets. The organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts before deploying any new devices in a networked environment.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) CIS Controls v7.1 - CIS CSC v7.1 4.2 Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.308(a)(5)(ii)(D) IRS Pub 1075 - IA-5(5) ISO/IEC 27002:2022 - 5(17) NIST SP 800-53 R4 IA-5(7)[S]{0} NIST SP 800-53 r5 - IA-5(7) PCI DSS v3.2.1 8.2.2 Supplemental Requirements - SR v6.4 20.2-0 Supplemental Requirements - SR v6.4 23.1-0 Supplemental Requirements - SR v6.4 6.2-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75
Level 2 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	Password settings are configured to not display passwords in plain (or clear) text by default.

	The organization: maintains a list of commonly-used, expected, or compromised passwords; updates the list of commonly-used, expected, or compromised passwords at least every 180 days; updates the list of commonly-used, expected, or compromised passwords when organizational passwords are suspected to have been compromised, either directly or indirectly; verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords; allows users to select long passwords and passphrases; allows users to select passwords and passphrases containing spaces and all printable characters; employs automated tools to assist the user in selecting strong passwords and authenticators.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 21 CFR Part 11.200(a) 21 CFR Part 11.3 21 CFR Part 11.300 AICPA Trust Services Criteria - AICPA 2017 CC6.6 Banking Requirements - FFIEC IS v2016 A.6.22(a) CIS Controls v7.1 - CIS CSC v7.1 16.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(01) (HIGH; MOD) FedRAMP - IA-5(7)[H] FedRAMP - IA-5(7)[M] FedRAMP - IA-6[H] FedRAMP - IA-6[L] FedRAMP - IA-6[M] Health Industry Cybersecurity Practices - 3.S.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.308(a)(5)(ii)(D) HITRUST IRS Pub 1075 - 2.B.3.4(3) IRS Pub 1075 - IA-5(1)a IRS Pub 1075 - IA-5(1)b IRS Pub 1075 - IA-5(1)c IRS Pub 1075 - IA-5(1)h4 IRS Pub 1075 - IA-5(7) IRS Pub 1075 - IA-6 ISO/IEC 27799:2016 9.2.4 ISO/IEC 27799:2016 9.3.1 ISO/IEC 27799:2016 9.4.2 ISO/IEC 27799:2016 9.4.3 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - IA-5(7) MARS-E v2.2 - IA-6 NIST Cybersecurity Framework v1.1 - RC.RP-1 NIST SP 800-171 r2 - 3.5.10[a] NIST SP 800-171 r2 - 3.5.10[b] NIST SP 800-171 r2 - 3.5.11[a] NIST SP 800-53 R4 IA-5(1)c[HML]{0} NIST SP 800-53 R4 IA-5(4)[S]{0} NIST SP 800-53 R4 IA-6[HML]{0} NIST SP 800-53 r5 - IA-5(1)a NIST SP 800-53 r5 - IA-5(1)b NIST SP 800-53 r5 - IA-5(1)c NIST SP 800-53 r5 - IA-5(1)e NIST SP 800-53 r5 - IA-5(1)f NIST SP 800-53 r5 - IA-5(1)g NIST SP 800-53 r5 - IA-5(1)h NIST SP 800-53 r5 - IA-5(18) NIST SP 800-53 r5 - IA-6 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)[IS.1e] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)[IS.1f] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)b NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)e NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)f NY OHIP Moderate-Plus Security Baseline v5.0 - IA-6 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-6[IS.1] PCI DSS v3.2.1 2.1

Level 2 Authoritative Source Mapping (Cont.):	PCI DSS v3.2.1 8.2.1 PCI DSS v3.2.1 8.2.2 PCI DSS v3.2.1 8.2.3 PCI DSS v3.2.1 8.2.4 PCI DSS v3.2.1 8.2.6 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(b) Supplemental Requirements - SR v6.4 22b-2 Supplemental Requirements - SR v6.4 22c-0 Supplemental Requirements - SR v6.4 23.2-0
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements
Level 3 Implementation (example):	Passwords are transmitted only when cryptographically-protected and stored using an approved hash algorithm and salt, preferably using a keyed hash.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC6.6 CIS Controls v7.1 - CIS CSC v7.1 16.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(01) (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(5)(ii)(D) IRS Pub 1075 - IA-5(1)d ISO/IEC 27799:2016 9.4.3 Legacy Inheritance Support - L.I.S. NIST SP 800-53 r5 - IA-5(1)d NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(1)d PCI DSS v3.2.1 8.2.5 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(b) Supplemental Requirements - SR v6.4 22a-0
Level CIS Implementation Requirements	
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization enforces the following minimum password requirements (User/Privileged): Minimum Password Age = 1/1; Maximum Password Age = 60/60; Minimum Password Length = 8/8; Password Complexity = 1/1 (minimum one (1) character from the four (4) character categories (A-Z, a-z, 0-9, special characters); and Password History Size = 6. The organization ensures PIV compliant access cards are valid for no longer than five years, and PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three years.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization enforces the following minimum password requirements: minimum password age = 1/1; maximum password age = 60/60; minimum password length = 12 characters; password complexity = at least one of each of upper-case letters, lower-case letters, numbers, and special characters; password history size = 6; at least one character be changed; and prohibit password reuse for 24 hours.

	The organization requires that quality passwords are used which are easy to remember, not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, telephone numbers, and dates of birth etc.), not vulnerable to dictionary attack (do not consist of words included in dictionaries), free of consecutive identical characters.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The information system, for password-based authentication, enforces password minimum lifetime restriction of one day, enforces non-privileged account passwords to be changed at least every 90 days, and enforces privileged account passwords to be changed at least every 60 days. Passwords are at least eight characters, easy to remember, not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, telephone numbers, and dates of birth), not vulnerable to dictionary attack (do not consist of words included in dictionaries), free of consecutive identical characters, and a combination of alphabetic, upper and lower case characters, numbers, and special characters (combination of any three of the above four listed is acceptable).
Level HIX Implementation Requirements	
Level HIX Implementation (example):	PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three years. The organization enforces the following minimum password requirements (user / privileged / process acting on behalf of a user): minimum password age = 1/1/1; maximum password age = 60/60/180; minimum password length = 8/8/15; password complexity = 1/1/3 (minimum one character, three for a process) from the four character categories (A-Z, a-z, 0-9, special characters); and password history size = 24/24/24. The information system uses password-protected initialization (boot) settings.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization requires that quality passwords are used which are at least seven characters long and contain both numeric and alphabetic characters. If password requirements can't be met, passwords/phrases must have a strength (entropy) at least equivalent to the parameters specified above. The organization changes passwords no less than every 90 days for regular and privileged (i.e., administrator) accounts.
Level Supplemental Requirements Implementation Requirements	

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system, for password-based authentication, meets or exceeds the following minimum password requirement: prohibits the use of dictionary names or words; MinimumPasswordAge = one [1] day; MaximumPasswordAge = sixty [60] days; MinimumPasswordLength = Minimum length of eight [8] characters for regular user passwords, and minimum length of fifteen [15] characters for administrators or privileged user passwords; PasswordComplexity = minimum (one [1] for Moderate) character(s) from the four [4] character categories (A-Z, a-z, 0-9, special characters); PasswordHistorySize = six [6] passwords for Moderate; minimum length (MinimumPasswordLength) for administrators or privileged users of fifteen [15] characters; if the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at six [6] for Moderate systems; store and transmit only encrypted representations of passwords; and allow the use of a temporary password for system logons with an immediate change to a permanent password.
Level NIST SP 800-171 Implementation Requirements	
Level NIST SP 800-171 Implementation (example):	The organization requires an immediate change to a permanent password when a temporary password is used for system logon.
Level State of MA Data Protection Act Implementation Requirements	
Level State of MA Data Protection Act Implementation (example):	Password policies, applicable to mobile devices, are documented, enforced through technical controls on all company devices or devices approved for BYOD usage, prohibit the changing of password/PIN lengths, and prohibit the changing of authentication requirements.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The information system, for password-based authentication: enforces minimum password complexity of a minimum of 12 characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters; enforces at least one changed character when new passwords are created; stores and transmits only encrypted representations of passwords; enforces lifetime restrictions of one day minimum and 60 day maximum; prohibits password reuse for 24 generations; and allows the use of a temporary password for system logons with an immediate change to a permanent password.

Control Reference: 01.e Review of User Access Rights

Control Specification:	All access rights shall be regularly reviewed by management via a formal documented process.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).

Level 1 Authoritative Source Mapping:	FedRAMP - AC-2j[L] FedRAMP - AC-2j[M] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(7)[NYS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(7)[NYS.3]

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	User access rights are reviewed after promotions, demotions, and termination of employment or end of other arrangement with a workforce member. User access rights are reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization (i.e., transfer). The organization maintains a documented list of authorized users of information assets.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) Banking Requirements - FFIEC IS v2016 A.6.20(c) Banking Requirements - FFIEC IS v2016 A.6.20(d) Banking Requirements - FFIEC IS v2016 A.6.22(c) Banking Requirements - FFIEC IS v2016 A.6.8(c) CIS Controls v7.1 - CIS CSC v7.1 16.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-05 (HIGH; MOD) COBIT 5 DS5.3 COBIT 5 DS5.4 COBIT 5 DSS05.04 FedRAMP - AC-2d[H] FedRAMP - AC-2d[L] FedRAMP - AC-2d[M] FedRAMP - CM-5(5)b[H] FedRAMP - CM-5(5)b[M] Health Industry Cybersecurity Practices - 3.M.B HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) IRS Pub 1075 - 2.B.3.3(3) IRS Pub 1075 - AC-2d1 IRS Pub 1075 - CM-12b IRS Pub 1075 - CM-5(5)b ISO/IEC 27002:2022 - 5(18) ISO/IEC 27799:2016 9.2.5 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-2d MARS-E v2.2 - AC-2j NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST SP 800-171 r2 - 3.1.1[a] NIST SP 800-171 r2 - 3.1.1[b] NIST SP 800-53 R4 AC-2j[HML]{2} NIST SP 800-53 R4 CM-5(5)b[S]{0} NIST SP 800-53 r5 - AC-2j NIST SP 800-53 r5 - CM-5(5)b NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2d1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(h) Supplemental Requirements - SR v6.4 19d-0
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization reviews all system accounts and disables any account that cannot be associated with a business process and owner. The organization monitors for dormant accounts, and notifies the user or user's manager of dormant accounts. The organization disables dormant accounts if not needed, or documents and monitors exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). The organization requires that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators are required to disable accounts that are not assigned to valid workforce members.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Authorized Access List (AAL) must be reviewed monthly or upon occurrence or potential indication of an event such as a possible security breach or personnel change. If there is any doubt of the identity of the individual, the security monitor must verify the identity of the individual against the Authorized Access List (AAL) prior to allowing entry into the restricted area.

	Management or a designee must maintain an authorized list of all personnel who have access to information system areas containing FTI.
Level HIE Implementation Requirements	
Level HIE Implementation (example):	The organization, acting as a Health Information Exchange (HIE), reviews user access every 90 days, for all employees and for all employees of connecting organizations, and reviews the appropriateness of each user's role every 90 days for all employees and for all employees of connecting organizations. Any discrepancies are remediated immediately following the review.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization inspects privileged accounts (e.g., administrator groups, root accounts, and other system-related accounts) on demand, and at least once every 14 days to ensure unauthorized accounts have not been created. Privileged user roles associated with applications are inspected every 30 days.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every 90 days to validate the need for such privileges, and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Objective Name: 01.03 User Responsibilities

Control Objective:	To prevent unauthorized user access, and compromise or theft of information and information assets.

Control Reference: 01.f Password Use

Control Specification:	Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of passwords and security of equipment.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA The Joint Commission v2016 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)

Level 1 Implementation (example):	The organization ensures users are made aware of the organization's password policies and requirements, are made aware to keep passwords confidential, avoid keeping a record (e.g., paper, software file, or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved, change passwords whenever there is any indication of possible system or password compromise, do not share individual user accounts or passwords, do not provide their password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks), do not use the same password for business and non-business purposes, and select quality passwords.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(5)(ii)(D) ISO/IEC 27002:2022 - 5(17) ISO/IEC 27799:2016 9.3.1 PCI DSS v3.2.1 8.2.5 PCI DSS v3.2.1 8.2.6 PCI DSS v3.2.1 8.4 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(b) The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA The Joint Commission v2016 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	If users need to access multiple services, systems, or platforms, and are required to maintain multiple separate passwords, they are advised that they may use a single, quality password for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system, or platform.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) FedRAMP - IA-5(8)[H] HIPAA Security Rule - § 164.308(a)(5)(ii)(D) ISO/IEC 27799:2016 9.3.1 NIST SP 800-53 R4 IA-5(8)[S]{0} NIST SP 800-53 r5 - IA-5(18) NIST SP 800-53 r5 - IA-5(8) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(b) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(e) The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Control Reference: 01.g Unattended User Equipment

Control Specification:	Users shall ensure that unattended equipment has appropriate protection.

Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA
Level 1 Implementation (example):	All users are made aware of: the security requirements and procedures for protecting unattended equipment; their responsibilities for terminating active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver); their responsibilities for logging-off mainframe computers, servers, and office PCs when the session is finished (e.g., not just switch off the PC screen or terminal); and their responsibilities for securing PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g., password access) when not in use.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-05 (HIGH; MOD) HIPAA Security Rule - § 164.316(b)(2)(ii) IRS Pub 1075 - 2.B.7.3(2)e ISO/IEC 27799:2016 11.2.8
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA High Moderate Supplemental
Level 2 Implementation (example):	The organization safeguards information system output devices (e.g., printers, monitors, copiers, scanners, facsimile machines) to help prevent unauthorized individuals from obtaining the output.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-05 (HIGH; MOD) FedRAMP - PE-5[H] FedRAMP - PE-5[M] HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - 2.B.2(3) IRS Pub 1075 - PE-5 MARS-E v2.2 - PE-5 NIST SP 800-53 R4 PE-5(1)[S]{0} NIST SP 800-53 R4 PE-5(2)a[S]{0} NIST SP 800-53 R4 PE-5[HM]{0} NIST SP 800-53 r5 - PE-5 NIST SP 800-53 r5 - PE-5(2) NY OHIP Moderate-Plus Security Baseline v5.0 - PE-5
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization secures keys, combinations, and other physical access devices.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization ensures that output from printers and fax machines are in a controlled area and secured when not in use. Physical access to monitors displaying FTI is controlled to prevent unauthorized access to the display output.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization ensures that SE laptops and third-party laptops that access or contain SE PPSI are powered down (i.e., shut down or hibernated) when unattended while outside of State facilities.

Control Reference: 01.h Clear Desk and Clear Screen Policy

Control Specification:	A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework Texas Medical Records Privacy Act

Level 1 Implementation (example):	Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use. Documents containing covered or critical information are removed from printers, copiers, and facsimile machines immediately. When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-11 (HIGH; MOD) HIPAA Security Rule - § 164.310(a)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Physical Security: General IRS Pub 1075 - PE-1(IRS-2) ISO/IEC 27002:2022 - 7(7) ISO/IEC 27799:2016 11.2.9

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)? No
Level 2 Regulatory Factors:	FISMA HITRUST De-ID Framework Texas Medical Records Privacy Act
Level 2 Implementation (example):	Covered or critical business information is not visible through envelope windows. Envelopes are marked according to their classification level (e.g., confidential). The organization ensures incoming mail points, outgoing mail points, and unattended facsimile machines are protected.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-03 (HIGH; MOD) HITRUST ISO/IEC 27799:2016 8.2.3

Objective Name: 01.04 Network Access Control

Control Objective:	To prevent unauthorized access to networked services.

Control Reference: 01.j User Authentication for External Connections

Control Specification:	Appropriate authentication methods shall be used to control access by remote users.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	

Level 1 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No
Level 1 Regulatory Factors:	FTC Red Flags Rule (16 CFR 681) HITRUST De-ID Framework High Low Moderate Supplemental
Level 1 Implementation (example):	Remote access by vendors and business partners (e.g., for remote maintenance) is disabled unless specifically authorized by management. Remote access to business partner accounts (e.g., remote maintenance) is immediately deactivated after use.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.24 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04 (HIGH; MOD) HITRUST De-ID Framework - De-ID Framework v1 Remote Access: Applicability NIST Cybersecurity Framework v1.1 - PR.MA-2 NIST SP 800-171 r2 - 3.7.5[b] NIST SP 800-53 R4 MA-4(7)[S]{0} NIST SP 800-53 R4 MA-4e[HML]{0} NIST SP 800-53 r5 - MA-4(7) NIST SP 800-53 r5 - MA-4e PCI DSS v3.2.1 12.3.9 PCI DSS v3.2.1 8.1.5
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)? No Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No Are wireless access points in place at any of the organization's in-scope facilities? No

Level 2 Regulatory Factors:	FTC Red Flags Rule (16 CFR 681) HITRUST De-ID Framework CA Civil Code § 1798.81.5 Supplemental Requirements High Moderate Supplemental
Level 2 Implementation (example):	The authentication of remote users is implemented using a password or passphrase and at least one of the following methods: a cryptographic based technique; biometric techniques; hardware tokens; software tokens; a challenge/response protocol; or, certificate agents. Dial-up connections are encrypted. If encryption is not used for dial-up connections, the CIO or his/her designated representative must provide specific written authorization.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.21(e) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.24 CIS Controls v7.1 - CIS CSC v7.1 12.11 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08(04) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04 (HIGH; MOD) FedRAMP - AC-18(1)[H] FedRAMP - AC-18(1)[M] FTC Red Flags Rule (16 CFR 681) - 681.A3.b Health Industry Cybersecurity Practices - 3.M.D HITRUST HITRUST De-ID Framework - De-ID Framework v1 Remote Access: Applicability IRS Pub 1075 - AC-18(1) MARS-E v2.2 - AC-18(1) NIST Cybersecurity Framework v1.1 - PR.AC-3 NIST SP 800-171 r2 - 3.1.17[a] NIST SP 800-53 R4 AC-17(4)b[HM]{0} NIST SP 800-53 R4 CP-13[S]{0} NIST SP 800-53 R4 MA-4(4)b[S]{1} NIST SP 800-53 r5 - CP-13 NIST SP 800-53 r5 - MA-4(4)b NY OHIP Moderate-Plus Security Baseline v5.0 - AC-18(1) PCI DSS v3.2.1 12.3.9 PCI DSS v3.2.1 8.1.5 PCI DSS v3.2.1 8.3.2 Supplemental Requirements - SR v6.4 13-0

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No
Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) Supplemental
Level 3 Implementation (example):	The organization's information system monitors and controls remote access methods. Remote administration sessions are authorized, encrypted, and employ increased security measures.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.24 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(04) (HIGH; MOD) FedRAMP - AC-17(1)[H] FedRAMP - AC-17(1)[M] IRS Pub 1075 - AC-17(1) MARS-E v2.2 - AC-17(1) NIST SP 800-171 r2 - 3.1.12[a] NIST SP 800-171 r2 - 3.1.12[b] NIST SP 800-171 r2 - 3.1.12[c] NIST SP 800-171 r2 - 3.1.12[d] NIST SP 800-171 r2 - 3.1.15[a] NIST SP 800-171 r2 - 3.1.15[b] NIST SP 800-171 r2 - 3.1.15[c] NIST SP 800-171 r2 - 3.1.15[d] NIST SP 800-53 R4 AC-17(1)[S]{0} NIST SP 800-53 r5 - AC-17(1)

Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization requires all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems, e.g., from an alternate work location or to sensitive information via a Web portal) to encrypt data in transit and use two-factor authentication.

Level CMS Implementation Requirements	
Level CMS Implementation (example):	If e-authentication is implemented as a remote access solution or associated with remote access, the organization ensures compliance with the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards. The organization requires callback capability with re-authentication to verify connections from authorized locations when the Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a User ID and password and enters the network through the standard authentication process. Access to such systems is authorized and logged. User IDs assigned to vendors will be recertified within every 365 days.
Level Federal Implementation Requirements	
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization provides the capability to expeditiously disconnect or disable remote access to the organization's system(s) within 15 minutes based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information system(s). The information system: accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies; accepts only federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials; employs only FICAM-approved information system components in information systems that authenticate non-organizational users; accepts third-party credentials; and conforms to FICAM-issued profiles.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	When FTI is being accessed remotely: encrypted modems and/or Virtual Private Networks (VPN) are required for every workstation and a smart card (microprocessor) for every user; smart cards have identification features; smart cards have authentication features; and smart cards provide data encryption. Two-factor authentication is required whenever FTI is being accessed from an alternate work location, or via the organization's web portal.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization incorporates multi-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third-parties (including vendor access for support and maintenance).

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization requires callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a User ID and password and enters the network through the standard authentication process. Access to such systems is authorized and logged. User IDs assigned to vendors will be recertified within every 365 days.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The system restricts remote network access based on organizational defined risk factors, e.g., time of day, location of access, physical location, network connection state, and measured properties of the current user and role.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization requires MFA protected VPN access be established before users are granted access to privileged servers.

Control Reference: 01.k Equipment Identification in Networks

Control Specification:	Automatic equipment identification shall be used as a means to authenticate connections from specific locations and equipment.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	HITRUST De-ID Framework GDPR High Moderate Supplemental
Level 1 Implementation (example):	The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection. Network devices that require authentication mechanisms use shared information (e.g., MAC or IP address) to control remote network access and access control lists to control remote network access.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.10 CIS Controls v7.1 - CIS CSC v7.1 11.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-20 (HIGH; MOD) FedRAMP - IA-3[H] FedRAMP - IA-3[M] Health Industry Cybersecurity Practices - 6.S.A IRS Pub 1075 - IA-3 ISO/IEC 27799:2016 13.1.3 MARS-E v2.2 - IA-3 NIST Cybersecurity Framework v1.1 - PR.AC-7 NIST SP 800-171 r2 - 3.1.1[c] NIST SP 800-171 r2 - 3.1.1[f] NIST SP 800-53 R4 IA-3(1)[S]{1} NIST SP 800-53 R4 IA-3(4)[S]{0} NIST SP 800-53 R4 IA-3[HM]{0} NIST SP 800-53 R4 IA-9[S]{1} NIST SP 800-53 r5 - IA-3(1) NIST SP 800-53 r5 - IA-3(4) NIST SP 800-53 r5 - IA-9 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-3 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-3[IS.1]

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	An identifier in or attached to equipment is used to indicate whether the equipment is permitted to connect to the network. The identifier used to indicate whether equipment is permitted to connect to the network clearly indicates which network the equipment is permitted to connect (if more than one network exists and, particularly, if these networks are of differing sensitivity). Physical protection of the equipment is required to maintain the security of the equipment identifier. The identifier is stored and transported in an encrypted format to protect it from unauthorized access.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) NIST SP 800-53 r5 - IA-4(9)

Control Reference: 01.l Remote Diagnostic and Configuration Port Protection

Control Specification:	Physical and logical access to diagnostic and configuration ports shall be controlled.
Factor Type:	Organizational

Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA
Level 1 Implementation (example):	Ports, services, and applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled or removed.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC6.1 CIS Controls v7.1 - CIS CSC v7.1 9.2 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 6.M.E Health Industry Cybersecurity Practices - 9.M.A IRS Pub 1075 - CM-7a IRS Pub 1075 - CM-7b1 IRS Pub 1075 - CM-7b3 MARS-E v2.2 - CM-7(1)b MARS-E v2.2 - CM-7b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(1)b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7a NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-7(1)[IS.1a] Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(d)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA

Level 2 Implementation (example):	Controls for the access to diagnostic and configuration ports includes the use of a key lock. Supporting procedures to control physical access to the port is implemented including ensuring that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04(03) (HIGH) COBIT 5 DS5.7 COBIT 5 DSS05.05
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP CA Civil Code § 1798.81.5 Supplemental Requirements CMS Minimum Security Requirements (High)
Level 3 Implementation (example):	The organization reviews the information system within 365 days to identify and disable unnecessary and non-secure functions, ports, protocols, and/or services. The organization identifies unauthorized software on the information system, employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized software on the information system, and reviews and updates the list of unauthorized software periodically but no less than annually.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 15.6 CIS Controls v7.1 - CIS CSC v7.1 9.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07(05) (HIGH) HIPAA Security Rule - § 164.308(a)(5)(ii)(B) NY OHIP Moderate-Plus Security Baseline v5.0 - CA-9[IS.1b] Supplemental Requirements - SR v6.4 6.6-0
Level CMS Implementation Requirements	
Level CMS Implementation (example):	A list of specifically needed system services, system ports, and system network protocols is maintained. A list of specifically needed system services, ports, and network protocols is documented in the security plan.

	If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization reviews the information system at least monthly to identify and disable unnecessary and non-secure functions, ports, protocols, and/or services. The organization employs automated mechanisms to prevent program execution in accordance with the list of authorized or unauthorized software programs, and rules authorizing the terms and conditions of software program usage. The organization: identifies defined software programs (defined in the applicable security plan) authorized to execute on the information system; employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and reviews and updates the list of authorized software programs at least quarterly or when there is a change.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Least functionality controls in place include disabling all unneeded network protocols, disabling all unneeded services, and assigning a dedicated static IP address to Multifunctional Devices (MFDs).
Level HICP Implementation Requirements	
Level HICP Implementation (example):	Access to network equipment is physically protected (e.g., a router must be stored in a room that is only accessible by authorized employees or contractors).
Control Reference: 01.m Segregation in Networks	
Control Specification:	Groups of information services, users, and information systems should be segregated on networks.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	PCI DSS v3.2.1 Supplemental Requirements High Supplemental
Level 1 Implementation (example):	Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of: enforcing security policies, being configured to filter traffic between these domains, and blocking unauthorized access in accordance with the organization's access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered and/or confidential information systems environment.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.6 Banking Requirements - FFIEC IS v2016 A.6.10 FedRAMP - AC-4(8)[H] FedRAMP - SC-7(21)[H] Health Industry Cybersecurity Practices - 6.M.A Health Industry Cybersecurity Practices - 6.M.B Health Industry Cybersecurity Practices - 6.M.E Health Industry Cybersecurity Practices - 6.S.A Health Industry Cybersecurity Practices - 6.S.B Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A IRS Pub 1075 - AC-18(IRS-1) IRS Pub 1075 - AC-4 IRS Pub 1075 - SC-7(4)h ISO/IEC 27799:2016 13.1.3 NIST Cybersecurity Framework v1.1 - PR.AC-5 NIST Cybersecurity Framework v1.1 - PR.DS-1 NIST SP 800-53 R4 AC-4(6)[S]{0} NIST SP 800-53 R4 AC-4(7)[S]{0} NIST SP 800-53 R4 AC-4(8)[S]{0} NIST SP 800-53 R4 SC-7(21)[H]{0} NIST SP 800-53 r5 - AC-4(6) NIST SP 800-53 r5 - AC-4(7) NIST SP 800-53 r5 - SC-50 NIST SP 800-53 r5 - SC-7(21) NIST SP 800-53 r5 - SC-7(27) PCI DSS v3.2.1 1.1 PCI DSS v3.2.1 1.1.4 Supplemental Requirements - SR v6.4 10.2-0
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	Networks are divided into separate logical network domains (e.g., an organization's internal network domains and external network domains) each protected by a defined security perimeter. Separate domains are implemented by controlling the network data flows using routing/switching capabilities, including access control lists, according to applicable flow control policies. The domains are defined based on a risk assessment and the different security requirements within each of the domains. A graduated set of controls is applied in different logical network domains to further segregate the network security environments (e.g., publicly accessible systems, internal networks; critical assets; and key information security tools, mechanisms, and support components associated with system and security administration). The organization implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. To ensure proper separation, the organization verifies any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, moves it to an internal VLAN and gives it a private address. The criteria for segregation of networks into domains is based on the access control policy and access requirements, and also takes account of the relative cost and performance impact of incorporating suitable network routing or gateway technology. Segregation of networks is based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption. Networks are segregated from production-level networks when migrating physical servers, applications, and data to virtualized servers.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.10 Banking Requirements - FFIEC IS v2016 A.6.17 CIS Controls v7.1 - CIS CSC v7.1 11.7 CIS Controls v7.1 - CIS CSC v7.1 14.1 CIS Controls v7.1 - CIS CSC v7.1 15.10 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(13) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-32 (HIGH) COBIT 5 DS5.10 COBIT 5 DSS05.02 FedRAMP - AC-4(21)[H] FedRAMP - AC-4(21)[M] FedRAMP - SC-7b[H] FedRAMP - SC-7b[L] FedRAMP - SC-7b[M] Health Industry Cybersecurity Practices - 6.M.A Health Industry Cybersecurity Practices - 6.S.A Health Industry Cybersecurity Practices - 9.M.E HIPAA Security Rule - § 164.310(a)(2)(ii) IRS Pub 1075 - SC-7b ISO/IEC 27002:2022 - 8(20) ISO/IEC 27799:2016 13.1.3 MARS-E v2.2 - AC-4(21) MARS-E v2.2 - SC-7(13) MARS-E v2.2 - SC-7b NIST Cybersecurity Framework v1.1 - PR.AC-5 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-171 r2 - 3.13.5[a] NIST SP 800-171 r2 - 3.13.5[b] NIST SP 800-53 R4 AC-4(2)[S]{0} NIST SP 800-53 R4 AC-4(21)[S]{0} NIST SP 800-53 R4 SC-7(22)[S]{0} NIST SP 800-53 R4 SC-7b[HML]{0} NIST SP 800-53 r5 - AC-4(2) NIST SP 800-53 r5 - AC-4(21) NIST SP 800-53 r5 - SC-7(22) NIST SP 800-53 r5 - SC-7(29) NIST SP 800-53 r5 - SC-7b NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7b PCI DSS v3.2.1 1.2
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization manages the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or on entirely different physical connectivity for management sessions for network devices. The organization segments the network based on the label or classification level of the information stored on the servers, ensuring all sensitive information is located on separated VLANs.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system isolates security functions from nonsecurity functions. The organization isolates organization-defined information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	If FTI in an 802.11 WLAN exists, the organization must architect the WLAN environment to provide logical separation between WLANs with different security profiles and from the wired LAN. The organization protects nonlocal maintenance sessions by separating the maintenance sessions from other network sessions with the system by either physically or logically separated communications paths.
Level HIX Implementation Requirements	
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system routes all remote accesses through a limited number of managed access control points. The organization must identify acceptable network access control points (e.g., connections standardized through the TIC initiative). In any situation where personally identifiable information (PII) is present, PII is stored on a logical or physical partition separate from the applications and software partition.

Control Reference: 01.n Network Connection Control

Control Specification:	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	State of Massachusetts Data Protection Act (201 CMR 17.00) High Moderate Supplemental
Level 1 Implementation (example):	At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception). The organization restricts the ability of users to connect to the internal network in accordance with the access control policy and the requirements of its business applications.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(05) (HIGH; MOD) FedRAMP - SC-7(5)[H] FedRAMP - SC-7(5)[M] Health Industry Cybersecurity Practices - 6.M.A Health Industry Cybersecurity Practices - 6.M.B Health Industry Cybersecurity Practices - 6.S.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.E IRS Pub 1075 - 3.3.6(2) MARS-E v2.2 - SC-7(5) NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-171 r2 - 3.13.6[a] NIST SP 800-171 r2 - 3.13.6[b] NIST SP 800-53 R4 SC-7(11)[S]{0} NIST SP 800-53 R4 SC-7(5)[HM]{0} NIST SP 800-53 r5 - SC-46 NIST SP 800-53 r5 - SC-7(11) NIST SP 800-53 r5 - SC-7(5) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(5) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(5)[IS.1] PCI DSS v3.2.1 1.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(6)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Community Supplemental Requirements 002 FedRAMP FISMA HITRUST De-ID Framework Supplemental Requirements CMS Minimum Security Requirements (High) GDPR High Low Moderate Supplemental

Level 2 Implementation (example):	The connection capability of users is restricted through network gateways (e.g., a firewall) that filter traffic by means of pre-defined tables or rules. Restrictions are applied to messaging (e.g., electronic mail); file transfer (e.g., peer-to-peer, FTP); interactive access (e.g., where a user provides input to the system); and common Windows applications. Linking network access rights to certain times of day or dates is implemented. The organization limits the number of external network connections to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. The organization implements a managed interface for each external telecommunication service (i.e., transmissions of data to or from other entities external to the secure site), including to other secure sites using networks or any other communications resources outside of the physical control of the secure site to transmit information. The organization establishes a traffic flow policy for each managed interface. The organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted. Security controls are implemented to secure the transmission of sensitive information. Transmissions of sensitive information over open, public networks are encrypted.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 16.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-02(11) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(04) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(07) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(08) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DSS05.02 Community Supplemental Requirements 002 - CSR002 v2018 11.2-1-3 FedRAMP - SC-7(3)[H] FedRAMP - SC-7(3)[M] FedRAMP - SC-7(4)a[H] FedRAMP - SC-7(4)a[M] FedRAMP - SC-7(4)b[H] FedRAMP - SC-7(4)b[M] FedRAMP - SC-7(4)d[H] FedRAMP - SC-7(4)d[M] FedRAMP - SC-7(4)e[M] FedRAMP - SC-7(7)[H] FedRAMP - SC-7(7)[M] FedRAMP - SC-7c[H] FedRAMP - SC-7c[L] FedRAMP - SC-7c[M] HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(1) HIPAA Security Rule - § 164.312(e)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Transmission Encryption: Policies IRS Pub 1075 - CM-7b4 IRS Pub 1075 - SC-7(3) IRS Pub 1075 - SC-7(4)a IRS Pub 1075 - SC-7(4)b IRS Pub 1075 - SC-7(7)a IRS Pub 1075 - SC-7(7)b1 IRS Pub 1075 - SC-7(7)b2 IRS Pub 1075 - SC-7(7)b3 IRS Pub 1075 - SC-7(7)c1 IRS Pub 1075 - SC-7(7)c2 IRS Pub 1075 - SC-7(7)c3 IRS Pub 1075 - SC-7(7)c4 IRS Pub 1075 - SC-7c ISO/IEC 27002:2022 - 5(14) MARS-E v2.2 - SC-7(3) MARS-E v2.2 - SC-7(4)a MARS-E v2.2 - SC-7(4)b MARS-E v2.2 - SC-7(4)c MARS-E v2.2 - SC-7(4)d MARS-E v2.2 - SC-7(4)e MARS-E v2.2 - SC-7(7) NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-171 r2 - 3.13.7[a] NIST SP 800-53 R4 AU-5(3)[S]{1} NIST SP 800-53 R4 CA-3(1)[S]{0} NIST SP 800-53 R4 CA-3(3)[S]{0} NIST SP 800-53 R4 SC-7(4)a[HM]{0} NIST SP 800-53 R4 SC-7(4)d[HM]{0} NIST SP 800-53 R4 SC-7(4)e[HM]{0}

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 R4 SC-7(7)[HM]{0} NIST SP 800-53 R4 SC-7c[HML]{0} NIST SP 800-53 r5 - AU-5(3) NIST SP 800-53 r5 - SC-7(3) NIST SP 800-53 r5 - SC-7(4)a NIST SP 800-53 r5 - SC-7(4)d NIST SP 800-53 r5 - SC-7(4)e NIST SP 800-53 r5 - SC-7(7) NIST SP 800-53 r5 - SC-7c NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(3) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1e] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)a NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)b NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)c NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)d NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)e NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(7) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(7)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7c NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(4)[PHI.1c] Supplemental Requirements - SR v6.4 42.1-0 Veterans Affairs Cybersecurity Program Directive 6500 - a(1)(d)

Level CIS Implementation Requirements

Level CMS Implementation Requirements

Level CMS Implementation (example):	The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces. The organization ensures NIST SP 800-46 guidelines are followed when supporting remote access (including teleworking), by defining policies and procedures for forms of permitted remote access, types of devices permissible for remote access, type of access remote users are granted, and how remote user account provisioning is handled.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. Remote access to the information system is authorized prior to allowing such connections. The organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	If using an external Web-based system or website that provides FTI over the Internet to a customer, the organization ensures access to the database through the Web application is limited by configuring the system architecture as a three-tier architecture with physically separate systems that provide layered security of the FTI.

Level HIX Implementation Requirements	

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP). The organization: monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative; establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; authorizes wireless access to the information system prior to allowing such connections; ensures that the CMS CIO must approve and distribute the overall wireless plan for his or her respective organization; and ensures that mobile and wireless devices, systems, and networks are not connected to wired HHS/CMS networks except through appropriate controls (e.g., VPN port) or unless specific authorization from HHS/CMS network management has been received.

Control Reference: 01.o Network Routing Control

Control Specification:	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High) High Moderate Supplemental

Level 1 Implementation (example):	The organization ensures that security gateways (e.g., a firewall) are used to validate source and destination addresses at internal and external network control points. The organization designs and implements network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The application-layer filtering proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a disallow list, or applying lists of allowed sites that can be accessed through the proxy while blocking all other sites. The organization forces outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Internal directory services and internal IP addresses are protected and hidden from any external access. Requirements for network routing control are based on the access control policy.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.6 CIS Controls v7.1 - CIS CSC v7.1 12.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07 (HIGH; MOD) Health Industry Cybersecurity Practices - 6.M.A Health Industry Cybersecurity Practices - 6.M.B Health Industry Cybersecurity Practices - 6.M.D Health Industry Cybersecurity Practices - 6.S.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A ISO/IEC 27799:2016 13.1.3 NIST SP 800-53 R4 CA-3(2)[S]{0} NIST SP 800-53 R4 CA-3(5)[HM]{0} NIST SP 800-53 R4 SC-30(5)[S]{0} NIST SP 800-53 R4 SC-7(16)[S]{0} NIST SP 800-53 R4 SC-7(9)a[S]{0} NIST SP 800-53 r5 - SC-30(5) NIST SP 800-53 r5 - SC-7(16) NIST SP 800-53 r5 - SC-7(9)a PCI DSS v3.2.1 1.2 PCI DSS v3.2.1 1.2.1
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	
Level 2 Authoritative Source Mapping:	
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization disables all workstation-to-workstation communication to limit an attacker’s ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs mechanisms capable of either decrypting content within encrypted communications for analysis or analyzing content before transmission/after receipt.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization blocks known malicious sites (inbound or outbound) at each Internet Access Point, within two business days following release of such sites from US-CERT, MS-ISAC or other sources.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The system: routes Internet traffic through a network intermediary device such as a content-filtering proxy server; prevents end-user systems from communicating directly to the Internet; does not solely rely on host-based controls to route Internet traffic; inspects encrypted Internet traffic; uses a reputation service to maintain an updated list of suspicious domains and URL strings; blocks malicious content, high-risk websites, and uncategorized websites; and analyzes traffic based on more criteria than domain name or IP, including URL, GETs, POSTs, content types (e.g., Flash), and user-agents.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization defines and employs tailored network boundary protections in addition to implementing commercially available solutions.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization uses an advanced protection technology to detect rewritten URLs at the time a URL is accessed in email messages.

Control Reference: 01.i Policy on the Use of Network Services

Control Specification:	Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. Authentication and authorization mechanisms shall be applied for users and equipment.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	

Level 1 Regulatory Factors:	Community Supplemental Requirements 002 FedRAMP Banking Requirements CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 1 Implementation (example):	The organization: determines who is allowed to access which network and networked services; specifies the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system); at a minimum, manages all enterprise devices remotely logging into the internal network, with remote control of their configuration; at a minimum, manages all enterprise devices remotely logging into the internal network, with installed software; at a minimum, manages all enterprise devices remotely logging into the internal network, with patch levels; publishes minimum security standards for access to the enterprise network by third-party devices (e.g., subcontractors/vendors); performs a security scan before allowing access; identifies the ports necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure; identifies the services necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure; and identifies the similar applications (e.g., protocols) necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(g) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.7(b) Banking Requirements - FFIEC IS v2016 A.6.7(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) Community Supplemental Requirements 002 - CSR002 v2018 11.2-3-2 Health Industry Cybersecurity Practices - 6.M.B Health Industry Cybersecurity Practices - 6.S.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.E ISO/IEC 27799:2016 9.1.2 NIST SP 800-53 R4 AC-17(6)[S]{2} NIST SP 800-53 R4 AC-17a[HML]{4} NIST SP 800-53 r5 - AC-17(6) NIST SP 800-53 r5 - AC-17a

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records

Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	The organization specifies the networks and network services users are authorized access. The organization ensures information systems or components of information systems for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants), and privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports) are identified as external information systems. The organization limits or prohibits the use of such external information systems by employees and other workforce members in accordance with organizational policy.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.7(a) CIS Controls v7.1 - CIS CSC v7.1 13.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) ISO/IEC 27799:2016 9.1.2 NIST Cybersecurity Framework v1.1 - ID.AM-4 NIST SP 800-53 R4 AC-20(4)[S]{2} NIST SP 800-53 r5 - AC-20(4) NIST SP 800-53 r5 - AC-20b
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The service provider uses the Center for Internet Security guidelines (Level 1) to establish a list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if United States Government Configuration Baseline (USGCB) is not available.

Objective Name: 01.05 Operating System Access Control

Control Objective:	To prevent unauthorized access to operating systems.

Control Reference: 01.p Secure Log-on Procedures

Control Specification:	Access to operating systems shall be controlled by a secure log-on procedure.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	A policy applicable to the organization's information systems addressing account lockout after consecutive unsuccessful login attempts is documented and enforced through technical controls.
Level 1 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 9.M.A NY OHIP Moderate-Plus Security Baseline v5.0 - AC-7a
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of users of the system(s) 500 to 5,500 Is the system(s) publicly positioned? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Does the system(s) transmit or receive data with a third-party? Yes
Level 2 Regulatory Factors:	CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements High Low Moderate
Level 2 Implementation (example):	Secure log-on procedure: will display a general notice warning that the computer is accessed by authorized users; will limit the number of unsuccessful log-on attempts allowed to six attempts; will enforce recording unsuccessful and successful attempts; will force a time delay of 30 minutes before further log-on attempts are allowed or rejecting any further attempts without specific authorization from an administrator; and will not display the password being entered by hiding the password characters with symbols. The procedure for logging into an operating system: is designed to minimize the opportunity for unauthorized access; discloses the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance; limits the number of unsuccessful log-on attempts allowed to three attempts; disconnects data link connections; sends an alarm message to the system console if the maximum number of log-on attempts is reached; sets the number of password retries in conjunction with the minimum length of the password and the value of the system being protected; limits the maximum and minimum time allowed for the log-on procedure, if exceeded, the system terminates the log-on; does not transmit usernames and passwords in clear text over the network; does not display system or application identifiers until the log-on process has been successfully completed; does not provide help messages during the log-on procedure that would aid an unauthorized user; and validates the log-on information only on completion of all input data. If an error condition arises during logons to an operating system, the system does not indicate which part of the data is correct or incorrect.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 16.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-09 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-12 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-06 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(5)(ii)(C) HIPAA Security Rule - § 164.308(a)(5)(ii)(D) ISO/IEC 27799:2016 9.4.2 NIST SP 800-53 R4 AC-7[HML]{0} NIST SP 800-53 r5 - AC-7 PCI DSS v3.2.1 8.1.6 PCI DSS v3.2.1 8.1.7 Supplemental Requirements - SR v6.4 20.1-0 Supplemental Requirements - SR v6.4 20.3-0 Supplemental Requirements - SR v6.4 7a.2-0
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	Is the system(s) accessible from the Internet? Yes
Level 3 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High)
Level 3 Implementation (example):	The organization configures the information system to lock out the user account automatically after three failed log-on attempts by a user during a one hour time period and requires the information system lock out to persist for a minimum of three hours. The number of concurrent sessions is limited to a specified number for all account types defined by the organization. Training includes reporting procedures and reporting responsibility for authorized users to report unauthorized log-ons and unauthorized attempts to log on.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-10 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-02 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(5)(ii)(C) HITRUST ISO/IEC 27799:2016 7.2.2 ISO/IEC 27799:2016 9.4.2 NIST Cybersecurity Framework v1.1 - RS.CO-2
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization configures the information system to lock out the user account automatically after three invalid login attempts during a 120-minute time window and requires the lock out to persist until released by an administrator. The organization configures the information system to lock out the user account automatically after three invalid login attempts through either a local or network connection during a 15-minute time window and requires the lock out to persist for a minimum of 30 minutes or until released by an administrator.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The number of concurrent network sessions for a user is limited and enforced to three sessions for privileged access and two sessions for non-privileged access. The information system purges/wipes information from organization-defined mobile devices based on organization-defined purging/wiping requirements/techniques after three consecutive, unsuccessful device logon attempts.
Level FTI Custodians Implementation Requirements	
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The information system limits the number of unsuccessful biometric logon attempts to three attempts. If the organization allows the use of authentication factors that are different from the primary authentication factors, it enforces a limit to the consecutive invalid logon attempts through use of the alternative factors by a user during a 24-hour period.
Level NIST SP 800-171 Implementation Requirements	
Level NIST SP 800-171 Implementation (example):	The organization enforces a limit of three consecutive invalid logon attempts by a user during a 15 minute period.

Control Reference: 01.q User Identification and Authentication

Control Specification:	All users shall have a unique identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	HITRUST De-ID Framework State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act
Level 1 Implementation (example):	Each user ID in the information system (including non-privileged, privileged, seeded, and service accounts) is assigned to a specific, named individual to maintain accountability. The organization requires multi-factor authentication for network and local access to privileged accounts.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 23 NYCRR 500 - 500.11(b)(1) 23 NYCRR 500 - 500.12(a) 23 NYCRR 500 - 500.12(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08 (HIGH; MOD) COBIT 5 DS5.3 COBIT 5 DSS05.04 FedRAMP - IA-2(1)[H] FedRAMP - IA-2(1)[M] FedRAMP - IA-2(3)[M] Health Industry Cybersecurity Practices - 1.M.B Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 3.M.A Health Industry Cybersecurity Practices - 3.M.D Health Industry Cybersecurity Practices - 3.S.A Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.312(a)(2)(i) IRS Pub 1075 - IA-12b IRS Pub 1075 - IA-2(1) ISO/IEC 27799:2016 9.2.1 ISO/IEC 27799:2016 9.2.3 MARS-E v2.2 - AC-17a MARS-E v2.2 - IA-2(1) MARS-E v2.2 - IA-2(2) MARS-E v2.2 - IA-2(3) NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST Cybersecurity Framework v1.1 - PR.AC-4 NIST Cybersecurity Framework v1.1 - PR.AC-6 NIST SP 800-171 r2 - 3.5.3[a] NIST SP 800-171 r2 - 3.5.3[b] NIST SP 800-171 r2 - 3.5.3[c] NIST SP 800-171 r2 - 3.5.3[d] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-12b NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2(1) NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2(1)[IS.1] PCI DSS v3.2.1 12.3.2 PCI DSS v3.2.1 8.1 PCI DSS v3.2.1 8.1.1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(a) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(b) Supplemental Requirements - SR v6.4 18.1-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	

Level 2 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No Is the system(s) accessible from the Internet? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No Are hardware tokens used as an authentication method within the scoped environment? No
Level 2 Regulatory Factors:	DirectTrust FISMA HITRUST De-ID Framework 23 NYCRR 500 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	Shared user/group IDs are only used in exceptional circumstances, where there is a clear business benefit for the use of a shared user ID for a group of users or a specific job. Approval by management is documented when shared user/group IDs are used. Additional controls are required to maintain accountability when shared user/group IDs are used. Generic IDs that are used by an individual are allowed only where the functions accessible or actions carried out by the ID do not need to be traced (e.g., read only access). The organization ensures that redundant user IDs are not issued to other users. Users are uniquely identified and authenticated for local access and remote access.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 21 CFR Part 11.100(a) 21 CFR Part 11.50(a) 21 CFR Part 11.50(b) 21 CFR Part 11.70 CIS Controls v7.1 - CIS CSC v7.1 11.5 CIS Controls v7.1 - CIS CSC v7.1 4.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(08) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(11) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(11) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-08 (HIGH; MOD) COBIT 5 DS5.3 COBIT 5 DSS05.04 FedRAMP - IA-2(1)[L] FedRAMP - IA-2(8)[H] FedRAMP - IA-2(8)[M] FedRAMP - IA-2[H] FedRAMP - IA-2[L] FedRAMP - IA-2[M] FedRAMP - IA-5(2)a[H] FedRAMP - IA-5(2)a[M] FedRAMP - IA-5(2)b[H] FedRAMP - IA-5(2)b[M] FedRAMP - IA-5(2)c[H] FedRAMP - IA-5(2)c[M] FedRAMP - IA-5(2)d[H] FedRAMP - IA-5(2)d[M] FedRAMP - IA-8[H] FedRAMP - IA-8[L] FedRAMP - IA-8[M] FTC Red Flags Rule (16 CFR 681) - 681.2c1.i FTC Red Flags Rule (16 CFR 681) - 681.2c2 Health Industry Cybersecurity Practices - 3.S.A Health Industry Cybersecurity Practices - 9.M.C HIPAA Security Rule - § 164.308(a)(5)(ii)(D) HIPAA Security Rule - § 164.312(a)(2)(i) HIPAA Security Rule - § 164.312(d) HITRUST De-ID Framework - De-ID Framework v1 Identification and Authentication (System-level): Authentication Policy HITRUST De-ID Framework - De-ID Framework v1 Identification and Authentication: Authentication Policy IRS Pub 1075 - IA-2 IRS Pub 1075 - IA-2(8) IRS Pub 1075 - IA-5(2)a1 IRS Pub 1075 - IA-5(2)a2 IRS Pub 1075 - IA-5(2)b1 IRS Pub 1075 - IA-5(2)b2 IRS Pub 1075 - IA-8 ISO/IEC 27799:2016 9.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - IA-2 MARS-E v2.2 - IA-2(8) MARS-E v2.2 - IA-5(2)a MARS-E v2.2 - IA-5(2)b

Level 2 Authoritative Source Mapping (Cont.):	MARS-E v2.2 - IA-5(2)c MARS-E v2.2 - IA-5(2)d MARS-E v2.2 - IA-8 NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST Cybersecurity Framework v1.1 - PR.AC-7 NIST SP 800-53 R4 AC-24(2)[S]{0} NIST SP 800-53 R4 AU-10(1)a[S]{2} NIST SP 800-53 R4 AU-10(2)[S]{2} NIST SP 800-53 R4 AU-10(4)[S]{2} NIST SP 800-53 R4 IA-10[S]{0} NIST SP 800-53 R4 IA-2(8)[HM]{0} NIST SP 800-53 R4 IA-2[HML]{0} NIST SP 800-53 R4 IA-4(1)[S]{0} NIST SP 800-53 R4 IA-5(13)[S]{1} NIST SP 800-53 R4 IA-5(14)[S]{0} NIST SP 800-53 R4 IA-5(2)[HM]{0} NIST SP 800-53 R4 IA-8[HML]{0} NIST SP 800-53 R4 SC-11(1)[S]{0} NIST SP 800-53 R4 SC-11[S]{0} NIST SP 800-53 R4 SC-7(15)[S]{0} NIST SP 800-53 r5 - AC-24(2) NIST SP 800-53 r5 - AU-10(1)a NIST SP 800-53 r5 - AU-10(2) NIST SP 800-53 r5 - AU-10(4) NIST SP 800-53 r5 - IA-10 NIST SP 800-53 r5 - IA-2 NIST SP 800-53 r5 - IA-2(8) NIST SP 800-53 r5 - IA-4(1) NIST SP 800-53 r5 - IA-5(13) NIST SP 800-53 r5 - IA-5(14) NIST SP 800-53 r5 - IA-5(2) NIST SP 800-53 r5 - IA-8 NIST SP 800-53 r5 - IA-8(5) NIST SP 800-53 r5 - IA-8(6) NIST SP 800-53 r5 - SA-8(6) NIST SP 800-53 r5 - SC-11 NIST SP 800-53 r5 - SC-11(1) NIST SP 800-53 r5 - SC-17b NIST SP 800-53 r5 - SC-7(15) NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)[IS.1a1] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)[IS.1a2] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)[IS.1b1] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)[IS.1b2] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)a1 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)a2 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)b1 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-5(2)b2 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-8 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-8[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - IA-8[IS.3] PCI DSS v3.2.1 12.3.2 PCI DSS v3.2.1 8.1 PCI DSS v3.2.1 8.1.1 PCI DSS v3.2.1 8.2.2 PCI DSS v3.2.1 8.3.2 PCI DSS v3.2.1 8.5

Level 2 Authoritative Source Mapping (Cont.):	PCI DSS v3.2.1 8.5.1 PCI DSS v3.2.1 8.6 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(a) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(2)(b) Supplemental Requirements - SR v6.4 7b.3-0
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No Is the system(s) accessible from the Internet? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes
Level 3 Regulatory Factors:	FedRAMP FISMA 23 NYCRR 500 CA Civil Code § 1798.81.5 Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	Electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners. The organization employs multifactor authentication for remote network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The organization employs multifactor authentication for local access to privileged accounts (including those used for non-local maintenance and diagnostic sessions).

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.200(b) CIS Controls v7.1 - CIS CSC v7.1 4.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(11) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02(12) (HIGH; MOD) FedRAMP - IA-2(11)[H] FedRAMP - IA-2(2)[H] FedRAMP - IA-2(2)[M] FedRAMP - IA-2(3)[H] FedRAMP - MA-4c[H] FedRAMP - MA-4c[L] FedRAMP - MA-4c[M] Health Industry Cybersecurity Practices - 1.S.A Health Industry Cybersecurity Practices - 3.M.D Health Industry Cybersecurity Practices - 3.S.A IRS Pub 1075 - IA-2(2) IRS Pub 1075 - MA-4(4)a IRS Pub 1075 - MA-4c MARS-E v2.2 - IA-2(11) NIST SP 800-53 R4 IA-2(1)[HML]{0} NIST SP 800-53 R4 IA-2(11)[HM]{1} NIST SP 800-53 R4 IA-2(2)[HM]{0} NIST SP 800-53 R4 IA-2(3)[HM]{0} NIST SP 800-53 R4 IA-2(6)[S]{1} NIST SP 800-53 R4 IA-2(7)[S]{1} NIST SP 800-53 R4 IA-5(12)[S]{0} NIST SP 800-53 R4 MA-4c[HML]{2} NIST SP 800-53 r5 - IA-2(1) NIST SP 800-53 r5 - IA-2(6) NIST SP 800-53 r5 - IA-5(12) NIST SP 800-53 r5 - IA-5(17) NIST SP 800-53 r5 - MA-4c NY OHIP Moderate-Plus Security Baseline v5.0 - IA-2(6)a Supplemental Requirements - SR v6.4 40-0 Supplemental Requirements - SR v6.4 49-0
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization requires access for all accounts, including those for network and security devices, to be obtained through a centralized point of authentication, for example, Active Directory or LDAP. All accounts have an expiration date that is monitored and enforced.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The information system uses multifactor authentication for local access to non-privileged accounts and replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps (e.g., Kerberos, TLS, etc.) for network access to privileged and non-privileged accounts. A risk assessment is used in determining the authentication needs of the organization.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization requires individuals to be authenticated with an individual authenticator as a second level of authentication when a group authenticator is employed. The organization manages individual identifiers, such as on personnel badges or email, by uniquely identifying each individual as an employee, contractor, volunteer, student, or other such organization-defined classification.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	If FTI is provided or shared through a publicly facing system, the organization implements strong identity proofing and authentication processes consistent with the latest guidance in the NIST SP 800-63 suite. The organization manages system identifiers by: receiving authorization from designated agency officials to assign an individual, group, role, service, or device identifier; selecting an identifier that identifies an individual, group, role, service, or device; assigning the identifier to the intended individual, group, role, service, or device; and preventing reuse of identifiers indefinitely.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The information system, for hardware token-based authentication, employs organization-specified mechanisms that satisfy generally acceptable minimum token requirements.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization does not use group, shared, or generic IDs, passwords, or other authentication methods. Generic user IDs are disabled or removed. Shared user IDs do not exist for system administration and other critical functions. Shared and generic user IDs are not used to administer any system components. Where other authentication mechanisms are used (e.g., physical or logical security tokens, smart cards, and certificates), use of these mechanisms are assigned as follows: authentication mechanisms must be assigned to an individual account and not shared among multiple accounts; and physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	Maintain individual ownership and accountability for use of all service accounts.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization requires the use of multifactor authentication for privileged access to administrative network zones. The organization manages access to all shared privileged accounts such that individual accountability is preserved and credentials are not synchronized across environments.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system implements organization-defined out-of-band authentication under organization-defined conditions.

	The organization ensures email cannot be used to transmit the random authenticator for the Out-of-Band (OOB) token.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization requires multi-factor authentication for access to non-privileged accounts.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	Multi-factor authentication is required for remote email access. The organization implements a federated Identity Access Management (IAM) solution to manage the credentials of all accounts.

Control Reference: 01.r Password Management System

Control Specification:	Systems for managing passwords shall be interactive and shall ensure quality passwords.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Is the system(s) accessible from the Internet? Yes Number of users of the system(s) 500 to 5,500 Is the system(s) publicly positioned? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Does the system(s) transmit or receive data with a third-party? Yes
Level 1 Regulatory Factors:	DirectTrust FedRAMP FISMA PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The password management system stores passwords in protected (e.g., encrypted or hashed) form, transmits passwords in protected (e.g., encrypted or hashed) form, stores password files separately from application system data, enforces a choice of quality passwords, enforces password changes, and maintains a record of previous user passwords and prevents re-use.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05(01) (HIGH; MOD) Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(5)(ii)(D) ISO/IEC 27799:2016 9.4.3 NIST SP 800-53 r5 - IA-5(18) PCI DSS v3.2.1 8.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(c)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust Supplemental Requirements Texas Medical Records Privacy Act
Level 2 Implementation (example):	The password management system requires the use of individual user IDs and passwords to maintain accountability, forces users to change temporary passwords at first log-on, does not display passwords on the screen when being entered, always changes vendor-supplied defaults before installing a system on the network, allows users to select and change their own passwords, and includes a confirmation procedure to allow for input errors.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-05 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(5)(ii)(D) ISO/IEC 27799:2016 9.2.4 ISO/IEC 27799:2016 9.4.3 PCI DSS v3.2.1 2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(1)(b) Supplemental Requirements - SR v6.4 6.4-0
Level CMS Implementation Requirements	
Level CMS Implementation (example):	If PKI-based authentication is used, the information system validates certificates by constructing a certification path with status information to an accepted trust anchor, enforces authorized access to the corresponding private key, and maps the authenticated identity to the user account.

Control Reference: 01.s Use of System Utilities

Control Specification:	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Supplemental
Level 1 Implementation (example):	The use of system utilities is controlled by implementing the following: implementing identification, authentication, and authorization procedures; segregating of system utilities from applications software; and limiting the of the use of system utilities to the minimum practical number of trusted, authorized users.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 AICPA Trust Services Criteria - AICPA 2017 CC6.2 Banking Requirements - FFIEC IS v2016 A.6.21(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) ISO/IEC 27799:2016 9.4.4 NIST SP 800-53 R4 MA-3(4)[S]{0} NIST SP 800-53 R4 SI-10(1)b[S]{0} NIST SP 800-53 r5 - MA-3(4) NIST SP 800-53 r5 - SI-10(1)b

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Is the system(s) publicly positioned? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Does the system(s) transmit or receive data with a third-party? Yes
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The use of system utilities is controlled by implementing authorization for ad hoc use of systems utilities, limiting the availability of system utilities (e.g., limitation of availability by setting restrictive file system level permissions for the access and execution of system utilities such as cmd.exe, ping, tracert, ipconfig, etc.), disabling of public “read” access to files, objects, and directories, logging of all use of system utilities, defining and documenting authorization levels for system utilities, the deletion of, or file system file execution permission denial of, all unnecessary software based utilities and system software, and the denial of system utilities availability to users who have access to applications on systems where segregation of duties is required. The information system owner regularly reviews the system utilities available to identify and eliminate unnecessary functions, such as scripts, drivers, features, subsystems, file systems, and unnecessary Web servers.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.21(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-03 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 ISO/IEC 27002:2022 - 8(18) ISO/IEC 27799:2016 9.4.4 MARS-E v2.2 - AC-3 PCI DSS v3.2.1 2.2.5 Supplemental Requirements - SR v6.4 6.3-2

Control Reference: 01.t Session Time-out

Control Specification:	Inactive sessions shall shut down after a defined period of inactivity.
Factor Type:	System

Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Texas Medical Records Privacy Act
Level 1 Implementation (example):	Both bring your own device (BYOD) and company-owned devices are configured to require an automatic session time-out screen as enforced through technical means.
Level 1 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 3.S.A Health Industry Cybersecurity Practices - 9.M.A
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) publicly positioned? Yes
Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Moderate
Level 2 Implementation (example):	The time-out system conceals information previously visible on the display with a publicly viewable image (e.g., a screen saver), pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish access using appropriate identification and authentication procedures. A time-out system (e.g., a screen saver) pauses the session screen after two minutes of inactivity, and closes network sessions after 30 minutes of inactivity.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) CIS Controls v7.1 - CIS CSC v7.1 16.11 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-11(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-12 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-10 (HIGH; MOD) FedRAMP - AC-11a[H] FedRAMP - AC-11a[M] FedRAMP - AC-11b[H] FedRAMP - AC-11b[M] HIPAA Security Rule - § 164.312(a)(2)(iii) IRS Pub 1075 - 2.B.7.3(2)e IRS Pub 1075 - AC-11a IRS Pub 1075 - AC-11b IRS Pub 1075 - AC-12 ISO/IEC 27799:2016 9.4.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-11a MARS-E v2.2 - AC-11b NIST SP 800-171 r2 - 3.1.10[a] NIST SP 800-171 r2 - 3.1.10[b] NIST SP 800-171 r2 - 3.1.10[c] NIST SP 800-171 r2 - 3.13.9[a] NIST SP 800-171 r2 - 3.13.9[b] NIST SP 800-171 r2 - 3.13.9[c] NIST SP 800-53 R4 AC-11[HM]{0} NIST SP 800-53 r5 - AC-11a PCI DSS v3.2.1 12.3.8 PCI DSS v3.2.1 8.1.8
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization requires that users log out when the time-period of expected inactivity exceeds 90 minutes, and at the end of the user's normal work period. The information system automatically terminates the network connection at the end of the session; otherwise, the system forcibly deallocates DHCP leases after seven days AND forcibly disconnects VPN connections after 30 minutes or less of inactivity.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system terminates the network connection associated with a communications session at the end of the session or after no longer than ten (10) minutes of inactivity for privileged sessions and no longer than fifteen (15) minutes of inactivity for user sessions. The information system terminates the network connection associated with a communications session at the end of the session or after no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions of inactivity.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization forcibly disconnects inactive VPN connections after 15 minutes of inactivity. The information system must automatically terminate a user session after 15 minutes of inactivity.

Level HIX Implementation Requirements	
Level HIX Implementation (example):	The information system automatically terminates the network connection associated with a communications session at the end of the session, or forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven days or other organization-defined time period and forcibly disconnects inactive Virtual Private Network (VPN) connections after 30 minutes of inactivity or other organization-defined time period.
Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	The time-out mechanism (e.g., screensaver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization restricts remote access sessions to last no longer than 24 hours. The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Control Reference: 01.u Limitation of Connection Time

Control Specification:	Restrictions on connection times shall be used to provide additional security for high-risk applications.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Connection time controls are implemented for sensitive computer applications, especially from high-risk locations (e.g., public, or external areas that are outside the organization's security management). Connection time controls include using predetermined time slots (e.g., for batch file transmissions or regular interactive sessions of short duration), restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation, and re-authentication at timed intervals.
Level 1 Authoritative Source Mapping:	21 CFR Part 11.10(d) Banking Requirements - FFIEC IS v2016 A.6.22(e) Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.312(a)(2)(iii) ISO/IEC 27799:2016 9.4.2

Objective Name: 01.06 Application and Information Access Control

Control Objective:	To prevent unauthorized access to information held in application systems.

Control Reference: 01.v Information Access Restriction

Control Specification:	Logical and physical access to information and application systems and functions by users and support personnel shall be restricted in accordance with the defined access control policy.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act Supplemental
Level 1 Implementation (example):	The requirements for controlling access to applications and application functions are addressed, such as, but not exclusive to: providing menus to control access to application system functions; controlling which data can be accessed by a particular user; controlling the access rights of users, e.g., read, write, delete and execute; controlling the access rights of other applications; limiting the information contained in outputs; and providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.22(b) Banking Requirements - FFIEC IS v2016 A.6.27(b) Banking Requirements - FFIEC IS v2016 A.6.8(a) Banking Requirements - FFIEC IS v2016 A.6.8(c) Banking Requirements - FFIEC IS v2016 A.8.1(k) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) Health Industry Cybersecurity Practices - 4.M.C HIPAA Security Rule - § 164.308(a)(4)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.312(a)(1) ISO/IEC 27799:2016 9.4.1 NIST SP 800-171 r2 - 3.1.2[a] NIST SP 800-171 r2 - 3.1.2[b] NIST SP 800-53 R4 AC-25[S]{0} NIST SP 800-53 R4 AC-3(3)[S]{2} NIST SP 800-53 r5 - AC-25 NIST SP 800-53 r5 - AC-3(15)b NIST SP 800-53 r5 - AC-3(3)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of users of the system(s) 500 to 5,500

Level 2 Regulatory Factors:	FISMA CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) GDPR High Low Moderate
Level 2 Implementation (example):	Access rights to other applications are controlled according to applicable access control policies. The organization ensures that outputs from application systems handling covered information contain only the information relevant to the use of the output, and are sent only to authorized terminals and locations.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.8.1(k) CIS Controls v7.1 - CIS CSC v7.1 14.6 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-14 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-15 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(4)(ii)(A) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(2)(ii) ISO/IEC 27799:2016 9.4.1 MARS-E v2.2 - AC-14c MARS-E v2.2 - AC-3 NIST SP 800-53 R4 AC-14a[HML]{0} NIST SP 800-53 r5 - AC-14a NY OHIP Moderate-Plus Security Baseline v5.0 - AC-14a

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No Is the system(s) accessible from the Internet? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes
Level 3 Regulatory Factors:	FedRAMP Banking Requirements PCI DSS v3.2.1
Level 3 Implementation (example):	When individuals are accessing sensitive information (e.g., covered information, cardholder data) from a remote location, then the copying, moving, printing, using print screen to capture, and storage of this information onto local hard drives and removable electronic media is prohibited, unless explicitly authorized for a defined business need.
Level 3 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 4.M.C HIPAA Security Rule - § 164.310(d)(1) PCI DSS v3.2.1 12.3.10

Level CMS Implementation Requirements	
Level CMS Implementation (example):	Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Access to FTI must be explicitly authorized strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. No person is given more FTI than is needed for performance of his/her duties. The organization ensures that only authorized users with a demonstrated need-to-know can query FTI data within a data warehouse.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	If there is an authorized business need to allow the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media for personnel accessing cardholder data via remote-access technologies, then the organization's usage policies require the data be protected in accordance with all applicable PCI DSS requirements. All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	Data stored in the information system is protected with system access controls and is encrypted when residing in non-secure areas. If wireless access is explicitly approved, the following wireless restrictions and access controls are implemented: Wireless device service set identifier broadcasting is disabled; Wireless encryption protection is enabled; Wireless access points are placed in secure areas; Wireless access points are shut down when not in use (i.e., nights, weekends); A stateful inspection firewall is implemented between the wireless network and the wired infrastructure; MAC address authentication is utilized for wireless access; Static IP addresses, not Dynamic Host Configuration Protocol (DHCP), are utilized for wireless access; Personal firewalls are utilized on all wireless clients; File sharing is disabled on all wireless clients; Intrusion detection agents are deployed on the wireless side of the firewall; Wireless activity is monitored and recorded, and the records are reviewed on a regular basis; Wireless activity adheres to CMS-CIO-POL-INF12-01, CMS Policy for Wireless Client Access; Wireless activity adheres to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN); Wireless printers and all Bluetooth devices such as keyboards are not allowed.

Control Reference: 01.w Sensitive System Isolation

Control Specification:	Sensitive systems shall have a dedicated and isolated computing environment.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Supplemental
Level 1 Implementation (example):	The sensitivity of an application is explicitly identified, and documented by the application/system owner.
Level 1 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-02 (HIGH; MOD) NIST SP 800-53 R4 AC-16b[S]{1} NIST SP 800-53 r5 - AC-16b
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Supplemental Requirements
Level 2 Implementation (example):	The sensitive application system runs on a dedicated computer, or only shares resources with trusted applications systems. Isolation is achieved using physical or logical methods. When a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks are identified, and accepted by the owner of the sensitive application.
Level 2 Authoritative Source Mapping:	
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	Number of users of the system(s) Greater than 5,500
Level 3 Regulatory Factors:	FedRAMP PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	System resources shared between two or more users are released back to the information system, and are protected from accidental or purposeful disclosure. Policy documents formally state that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Requirements have been defined for maintaining a separate execution domain for each executing process.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-04 (HIGH; MOD) FedRAMP - SC-39[H] FedRAMP - SC-39[L] FedRAMP - SC-39[M] FedRAMP - SC-4[H] FedRAMP - SC-4[M] IRS Pub 1075 - SC-39 IRS Pub 1075 - SC-4 MARS-E v2.2 - SC-39 MARS-E v2.2 - SC-4 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-171 r2 - 3.13.4[a] NIST SP 800-53 R4 SC-3(1)[S]{0} NIST SP 800-53 R4 SC-39(1)[S]{0} NIST SP 800-53 R4 SC-39(2)[S]{0} NIST SP 800-53 R4 SC-39[HML]{0} NIST SP 800-53 R4 SC-4[HM]{0} NIST SP 800-53 r5 - SC-3(1) NIST SP 800-53 r5 - SC-39 NIST SP 800-53 r5 - SC-39(1) NIST SP 800-53 r5 - SC-39(2) NIST SP 800-53 r5 - SC-4 NY OHIP Moderate-Plus Security Baseline v5.0 - SC-39 NY OHIP Moderate-Plus Security Baseline v5.0 - SC-39[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-4 NY OHIP Moderate-Plus Security Baseline v5.0 - SC-4[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-4[PHI.1]
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs boundary protection mechanisms to separate defined information system components (defined in the applicable security plan) supporting CMS missions and/or business functions. The organization ensures that system resources shared between two or more users are released back to the information system and protected from accidental or purposeful disclosure.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	When authorization to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. Bulk record identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.
Level HIX Implementation Requirements	
Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	The organization ensures sensitive applications and information are segregated from other customer's or supplier's own application or information by using logical access controls and/or physical access controls.

Objective Name: 01.07 Mobile Computing and Teleworking

Control Objective:	To ensure the security of information when using mobile computing devices and teleworking facilities.

Control Reference: 01.x Mobile Computing and Communications

Control Specification:	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication devices.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Do any of the organization's personnel travel to locations the organization deems to be of significant risk? No
Level 1 Regulatory Factors:	FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 1 Implementation (example):	The organization monitors for unauthorized connections of mobile devices. Individuals are issued specifically configured mobile devices for travel to locations the organization deems to be of significant risk in accordance with organizational policies and procedures. Upon return from these locations the devices are checked for malware and physical tampering.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) Banking Requirements - FFIEC IS v2016 A.6.24 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-19 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(07) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04 (HIGH; MOD) FedRAMP - AC-19(5)[H] FedRAMP - AC-19(5)[M] FedRAMP - CM-2(7)a[H] FedRAMP - CM-2(7)a[M] FedRAMP - CM-2(7)b[H] FedRAMP - CM-2(7)b[M] Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 4.M.C Health Industry Cybersecurity Practices - 4.S.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.312(a)(2)(iv) IRS Pub 1075 - 2.C.7(3) IRS Pub 1075 - 2.C.7(4) IRS Pub 1075 - 2.C.7(5) IRS Pub 1075 - CM-2(7)a IRS Pub 1075 - CM-2(7)b MARS-E v2.2 - CM-2(7)a MARS-E v2.2 - CM-2(7)b NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - PR.AC-3 NIST SP 800-171 r2 - 3.1.18[a] NIST SP 800-171 r2 - 3.1.18[b] NIST SP 800-171 r2 - 3.1.18[c] NIST SP 800-171 r2 - 3.1.19[a] NIST SP 800-171 r2 - 3.1.19[b] NIST SP 800-53 R4 AC-19(4)a[S]{2} NIST SP 800-53 R4 AC-19(4)b[S]{1} NIST SP 800-53 R4 CM-2(7)[HM]{0} NIST SP 800-53 R4 MP-7(2)[S]{0} NIST SP 800-53 r5 - AC-19(4)a NIST SP 800-53 r5 - AC-19(4)b1 NIST SP 800-53 r5 - CM-2(7) NIST SP 800-53 r5 - MP-7(2) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-2(7)a NY OHIP Moderate-Plus Security Baseline v5.0 - CM-2(7)b Supplemental Requirements - SR v6.4 38d-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records

Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The organization uses full-disk encryption to protect the confidentiality of information on laptops and other mobile devices that support full-disk encryption and is enforced through technical controls. A mobile computing policy is developed which includes: The mobile computing policy includes the organization's definition of mobile devices; The mobile computing policy includes acceptable usage; The mobile computing policy includes requirements for physical protection; The mobile computing policy includes requirements for access controls; The mobile computing policy includes requirements for cryptographic techniques; The mobile computing policy includes requirements for back-ups; The mobile computing policy includes requirements for virus protection; The organization installs personal firewall software or equivalent functionality on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network; Mobile computing devices are physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers, and meeting places; The organization only authorizes connections of mobile devices meeting organizational usage restrictions, configuration requirements, connection requirements, and implementation guidance; [and which] enforce requirements for the connection of mobile devices to sensitive information systems; and Information system functionality on mobile devices that provides the capability for automatic execution of code without user direction is disabled. Users of mobile computing devices in public places take care to avoid the risk of overlooking by unauthorized persons. Training is arranged for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that are implemented.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.15(a)(1) 23 NYCRR 500 - 500.15(a)(2) 23 NYCRR 500 - 500.15(b) Banking Requirements - FFIEC IS v2016 A.6.24 CIS Controls v7.1 - CIS CSC v7.1 12.12 CIS Controls v7.1 - CIS CSC v7.1 13.6 CIS Controls v7.1 - CIS CSC v7.1 8.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-19 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-19(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04 (HIGH; MOD) FedRAMP - AC-19a[H] FedRAMP - AC-19a[L] FedRAMP - AC-19a[M] FedRAMP - AC-19b[H] FedRAMP - AC-19b[L] FedRAMP - AC-19b[M] Health Industry Cybersecurity Practices - 2.L.B HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(e)(2)(ii) IRS Pub 1075 - 3.3.4(1) IRS Pub 1075 - AC-19a IRS Pub 1075 - AC-19b ISO/IEC 27799:2016 6.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-17a NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - PR.AC-3 NIST SP 800-53 R4 AC-19(4)b[S]{3} NIST SP 800-53 R4 AC-19(4)b[S]{5} NIST SP 800-53 R4 AC-19(4)c[S]{0} NIST SP 800-53 R4 AC-19(5)[HM]{0} NIST SP 800-53 R4 AC-19[HML]{0} NIST SP 800-53 R4 SA-18(2)[S]{1} NIST SP 800-53 r5 - AC-19 NIST SP 800-53 r5 - AC-19(4)b1 NIST SP 800-53 r5 - AC-19(4)b2 NIST SP 800-53 r5 - AC-19(4)b4 NIST SP 800-53 r5 - AC-19(4)c NIST SP 800-53 r5 - AC-19(5) NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6(8) NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6(8)[IS.1] PCI DSS v3.2.1 1.4 PCI DSS v3.2.1 9.5 Supplemental Requirements - SR v6.4 38a-0 Supplemental Requirements - SR v6.4 38b-0 Supplemental Requirements - SR v6.4 38c-0 Supplemental Requirements - SR v6.4 39a-0 Supplemental Requirements - SR v6.4 39b-0
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The CIO, or his/her designated representative, authorizes the connection of mobile devices to organizational information systems. The organization requires that the use of contractor-owned devices is documented within the contract and the system security plan, requires employing information security and privacy protections appropriate for the sensitivity of the data, and is approved by the Authorizing Official (AO) in advance.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization purges/wipes information from mobile devices (e.g., personal digital assistants, smartphones, tablets), excluding laptops, after 10 consecutive, unsuccessful logon attempts. When FTI is used in a mobile device environment, mobile device management controls are in place that include security policies, security procedures, inventories of all mobile devices accessing FTI, and standardized security configurations for all mobile devices. An annual risk assessment is conducted on the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI. Protection mechanisms are in place in case a mobile device is lost or stolen. All data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards. All data communication with the organization's internal network is encrypted using a cryptographic module that is FIPS 140-2 compliant. The organization must control end-user ability to download only authorized applications to the device and must limit the accessibility to FTI by applications to only authorized applications. All mobile device management servers that receive, process, store, or transmit FTI are hardened. A centralized mobile device management solution is used to authenticate organization-issued and personally owned mobile devices prior to allowing access to the internal network. Security events are logged for all mobile devices and the mobile device management server. The organization disables wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, is disabled to the extent possible. Disposal of all mobile device component hardware follows the same media sanitization and disposal procedures as other media.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization: Authorizes the connection of mobile devices to organizational information systems through the CIO; Only allows the use of organization-owned mobile devices and software to process, access and store personally identifiable information (PII); Employs an approved method of cryptography to protect PII residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops; Enforces requirements for the connection of mobile devices to information systems; Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, and installing virus protection software.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization purges/wipes information from organization-defined mobile devices based on organization-defined purging/wiping requirements/techniques after an organization-defined number of consecutive, unsuccessful device logon attempts. Full disk encryption is required for all State-issued laptops that access or contain SE information. Full disk encryption products use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.

Control Reference: 01.y Teleworking

Control Specification:	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.

Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA
Level 1 Implementation (example):	Suitable protection of the teleworking site is in place to protect against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems, or misuse of facilities. Prior to authorizing teleworking: the physical security of the teleworking site is evaluated (e.g., of the building and local environment), and threats/issues associated with the physical security of the teleworking site are addressed.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.24 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-17 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - 2.B.7.3(2)d IRS Pub 1075 - PE-17b IRS Pub 1075 - PE-17c ISO/IEC 27002:2022 - 6(7) ISO/IEC 27799:2016 6.2.1 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST SP 800-171 r2 - 3.10.6[a] NIST SP 800-171 r2 - 3.10.6[b] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-17b
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	

Level 2 Regulatory Factors:	FISMA High Low Moderate
Level 2 Implementation (example):	Teleworking activities are formally managed/controlled, and only authorized if suitable security arrangements and security controls that comply with relevant security policies and organizational requirements are in place. Communications security requirements address the: need for remote access to the organization's internal systems; sensitivity of information that will be accessed and that will be accessed and pass over the communication link; and sensitivity of the internal system. The use of home networks and requirements/restrictions on the configuration of wireless network services including encryption (AES WPA2 at a minimum) are addressed with respect to teleworking arrangements. Antivirus protection with respect to teleworking arrangements is addressed. Operating system patching with respect to teleworking arrangements is addressed. Application patching with respect to teleworking arrangements is addressed. Firewall requirements consistent with corporate policy are addressed with respect to teleworking arrangements. Revocation of authority and access rights with respect to teleworking arrangements is addressed. The return of equipment when the teleworking activities are terminated is addressed. Verifiable unique IDs are required for all teleworkers accessing the organization's network via a remote connection. The connection between the organization and the teleworker's location is secured via an encrypted channel. The organization maintains ownership over the assets used by teleworkers in order to achieve the requirements of this control. Prior to teleworking authorization, personnel who telework are trained on: security awareness, privacy, and teleworker responsibilities.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.24 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-02 (HIGH; MOD) ISO/IEC 27799:2016 6.2.2 NIST SP 800-53 R4 AC-17a[HML]{2} NIST SP 800-53 R4 PE-17b[HM]{0} NIST SP 800-53 r5 - AC-17a NIST SP 800-53 r5 - PE-17a NIST SP 800-53 r5 - PE-17c NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3(5)[IS.7]

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No

Level 3 Regulatory Factors:	DirectTrust EHNAC FedRAMP CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	Prior to authorizing teleworking, the following matter is addressed: a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access; the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed; the provision of suitable communication equipment, including methods for securing remote access; rules and guidance on family and visitor access to equipment and information; the provision of hardware and software support and maintenance; the procedures for back-up and business continuity; the provision of a means for teleworkers to communicate with information security personnel in case of security incidents or problems; audit and security monitoring; and any organization-owned equipment is used only for business purposes by authorized employees. The organization has provided additional insurance to address the risks of teleworking.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-17 (HIGH; MOD) FedRAMP - PE-17a[H] FedRAMP - PE-17a[M] FedRAMP - PE-17b[H] FedRAMP - PE-17b[M] FedRAMP - PE-17c[H] FedRAMP - PE-17c[M] HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - 2.B.7.3(2)d IRS Pub 1075 - PE-17a ISO/IEC 27799:2016 6.2.2 MARS-E v2.2 - AC-20a1 MARS-E v2.2 - PE-17a MARS-E v2.2 - PE-17b MARS-E v2.2 - PE-17c NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-53 R4 AC-17b[HML]{0} NIST SP 800-53 R4 AU-14(3)[S]{1} NIST SP 800-53 R4 PE-17a[HM]{0} NIST SP 800-53 R4 PE-17c[HM]{2} NIST SP 800-53 r5 - AC-17(4)b NIST SP 800-53 r5 - AC-17b NIST SP 800-53 r5 - AU-14(3) NIST SP 800-53 r5 - PE-17b NIST SP 800-53 r5 - PE-17d NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-17a NY OHIP Moderate-Plus Security Baseline v5.0 - PE-17b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-17c NY OHIP Moderate-Plus Security Baseline v5.0 - PE-17d

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	When FTI is accessed at alternative worksites, such as an employee's home or other non-traditional worksites, the alternative worksites remain subject to the same safeguard requirements as the organization's offices and the highest level of attainable security. The organization addresses how it will meet its minimum protection standards for FTI at alternate worksites (e.g., employee's homes or other non-traditional worksites). The organization conducts and fully documents periodic inspections of alternative worksites during the year to ensure that safeguards are adequate. The organization retains ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate worksites.

Control Category: 02.0 - Human Resources Security

Objective Name: 02.01 Prior to Employment

Control Objective:	To ensure that employees, contractors, and third-party users are suitable for the roles for which they are being considered, to reduce the risk of fraud, theft, or misuse of facilities.

Control Reference: 02.a Roles and Responsibilities

Control Specification:	Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the organization's information security policy.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	PCI DSS v3.2.1
Level 1 Implementation (example):	Policies and/or standards related to user roles and responsibilities include: implementing and acting in accordance with the organization's information security policies; protecting assets from unauthorized access, disclosure, modification, destruction, or interference; executing particular security processes or activities; ensuring responsibility is assigned to the individual for actions taken; reporting security events or potential events or other security risks to the organization; and security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 23 NYCRR 500 - 500.18 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.9 Health Industry Cybersecurity Practices - 10.M.A Health Industry Cybersecurity Practices - 10.S.A HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) IRS Pub 1075 - 3.3.5(1)a IRS Pub 1075 - 3.3.5(1)b ISO/IEC 27002:2022 - 5(10) ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 7.1.2 NIST Cybersecurity Framework v1.1 - DE.DP-1 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST SP 800-53 r5 - PL-2a4 NIST SP 800-53 r5 - PS-9
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The organization has developed, disseminated, and annually reviewed and updated a formal, documented personnel security plan. The formal, documented personnel security policy addresses the purpose of its human resources security protection program, the scope of its human resources security protection program, the roles of its human resources security protection program, the responsibilities for its human resources security protection program, management commitment to its human resources security protection program, coordination among organizational entities for its human resources security protection program, and compliance with its human resources security protection program. Further, the organization documents procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

	The organization assigns risk designations to all organizational positions as appropriate, establishes screening criteria for risk designations as appropriate, and reviews and revises designations every 365 days.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.4 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-02 (HIGH; MOD) FedRAMP - PS-2a[H] FedRAMP - PS-2a[L] FedRAMP - PS-2a[M] FedRAMP - PS-2b[H] FedRAMP - PS-2b[L] FedRAMP - PS-2c[H] FedRAMP - PS-2c[L] FedRAMP - PS-2c[M] FedRAMP - PS-3(3)b[M] HIPAA Privacy Rule - 164.530(a)(2) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 7.1.2 MARS-E v2.2 - PS-2a MARS-E v2.2 - PS-2b MARS-E v2.2 - PS-2e NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST SP 800-53 R4 PS-2[HML]{0} NIST SP 800-53 R4 PS-3(3)b[S]{0} NIST SP 800-53 R4 PS-6(2)c[S]{2} NIST SP 800-53 R4 SA-21(1)[S]{0} NIST SP 800-53 r5 - PS-2 NIST SP 800-53 r5 - PS-3(3)b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-2a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-2b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-2d NY OHIP Moderate-Plus Security Baseline v5.0 - PS-2e PCI DSS v3.2.1 12.4.1
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization assigns a risk designation to all organizational positions, establishes screening criteria for individuals filling those positions, and reviews and updates position risk designations when recruitment actions are taken or when position descriptions are rewritten. The organization incorporates security and privacy roles and responsibilities into organizational position descriptions.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	Data Governance roles and responsibilities such as Data Producers, Data Consumers, Data Custodians, Data Stewards, and stakeholders are defined and documented.

Control Reference: 02.b Screening

Control Specification:	Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	PCI DSS v3.2.1 High Low Moderate Supplemental
Level 1 Implementation (example):	The organization screens individuals requiring access to organizational information before authorizing access.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.8(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-03 (HIGH; MOD) FedRAMP - PS-3(3)b[H] FedRAMP - PS-3(3)b[M] FedRAMP - PS-3a[H] FedRAMP - PS-3a[L] FedRAMP - PS-3a[M] HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.312(d) IRS Pub 1075 - PS-3a ISO/IEC 27799:2016 7.1.1 MARS-E v2.2 - PS-3a MARS-E v2.2 - PS-3e1 MARS-E v2.2 - PS-5a NIST SP 800-171 r2 - 3.9.1[a] NIST SP 800-53 R4 PS-3a[HML]{0} NIST SP 800-53 R4 SA-21[S]{2} NIST SP 800-53 r5 - PS-3a NIST SP 800-53 r5 - SA-21a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3[IS.4a] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3e1 PCI DSS v3.2.1 12.7

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	Where a job, either on initial appointment or on promotion, involves the person having access to information assets and, in particular, those handling covered information (e.g., financial information, personal information, or highly confidential information), the organization verifies the identity of such staff, current address of such staff, and previous employment of such staff. The organization defines criteria and limitations for verification checks (e.g., who is eligible to screen people, and how, when, and why verification checks are carried out).

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.4 Banking Requirements - FFIEC IS v2016 A.6.8(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-03 (HIGH; MOD) HIPAA Privacy Rule - 164.504(e)(2)(ii)(D) HIPAA Privacy Rule - 164.530(i)(3) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) ISO/IEC 27002:2022 - 6(1) ISO/IEC 27799:2016 7.1.1 MARS-E v2.2 - PS-2d MARS-E v2.2 - PS-3a MARS-E v2.2 - PS-3b MARS-E v2.2 - PS-3c MARS-E v2.2 - PS-3d NIST Cybersecurity Framework v1.1 - ID.GV-3 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST Cybersecurity Framework v1.1 - RC.CO-1 NIST Cybersecurity Framework v1.1 - RC.CO-2 NIST Cybersecurity Framework v1.1 - RC.CO-3 NIST SP 800-53 R4 PS-3b[HML]{0} NIST SP 800-53 R4 SI-12[HML]{2} NIST SP 800-53 r5 - PS-3b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3(3)b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-3d NY OHIP Moderate-Plus Security Baseline v5.0 - PS-5[PRIV.1] PCI DSS v3.2.1 12.7
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP Banking Requirements PCI DSS v3.2.1 Supplemental

Level 3 Implementation (example):	Verification checks consider all relevant: privacy legislation; protection of covered data legislation; and employment-based legislation. Where permitted and appropriate, verification checks: include availability of satisfactory character references (e.g., one business and one personal); include a completeness and accuracy check of the applicant's curriculum vitae; include confirmation of claimed academic and professional qualifications; include independent identity check (passport or similar document); and require all applicants to complete an I-9 form to verify that they are eligible to work in the United States. Verification checks are completed prior to granting access to covered and/or confidential information. The organization specifically defines an individual who performs all screening checks, documents and maintains a list of all screened applicants, and confirms each applicant is assigned a risk.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.8(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-03 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HITRUST ISO/IEC 27799:2016 7.1.1 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST SP 800-53 R4 IA-4(3)[S]{1} NIST SP 800-53 r5 - PS-3(3)b NIST SP 800-53 r5 - PS-3(4) PCI DSS v3.2.1 12.7
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization: requires that individuals with significant security responsibilities be assigned; requires that individuals with significant security responsibilities hold, at a minimum, Tier 2S background investigation as defined in the HHS Personnel Security/Suitability Handbook; and assigns other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook. The organization requires that personnel security policies and procedures must address the different levels of background investigations, or other personnel security requirements, necessary to access different levels of PII.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	Rescreening is required during the 5th year for top secret security clearance, 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization initiates a background investigation for all newly hired employees, contractors, and sub-contractors who will require access to FTI to perform assigned duties. Background investigations for any individual granted access to FTI include, at a minimum, FBI fingerprinting (FD-258); check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the prior five years, and if applicable, of the appropriate agency for any identified arrests; and citizenship/residency. The organization establishes a written background investigation policy that conforms to the standards of Publication 1075. Organizations must ensure a reinvestigation is conducted within five years from the date of the previous background investigation for each employee, contractor, and sub-contractor requiring access to FTI.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization ensures that individuals with significant security responsibilities possess, at a minimum, a Level 5 Public Trust.

Objective Name: 02.02 During On-Boarding

Control Objective:	To ensure agreements are signed by employees, contractors, and third-party users of information assets on their security roles and responsibilities at the time of their employment or engagement, prior to access being granted.

Control Reference: 02.c Terms and Conditions of Employment

Control Specification:	As part of their contractual obligation, employees, contractors, and third-party users shall agree and sign the terms and conditions of their employment contract, which shall include their responsibilities for information security.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High) Supplemental
Level 1 Implementation (example):	The organization ensures that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The organization develops and documents access agreements for organizational systems. Privileges are not granted until the terms and conditions have been satisfied and agreements have been signed.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(l) 23 NYCRR 500 - 500.11(a)(1) 23 NYCRR 500 - 500.11(a)(2) 23 NYCRR 500 - 500.11(a)(3) 23 NYCRR 500 - 500.11(b)(1) 23 NYCRR 500 - 500.11(b)(2) 23 NYCRR 500 - 500.11(b)(3) 23 NYCRR 500 - 500.11(b)(4) 23 NYCRR 500 - 500.11(c) Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-06 (HIGH; MOD) FedRAMP - PS-6a[H] FedRAMP - PS-6a[L] FedRAMP - PS-6a[M] IRS Pub 1075 - PS-6a ISO/IEC 27002:2022 - 6(2) ISO/IEC 27799:2016 7.1.2 MARS-E v2.2 - PS-3e2 MARS-E v2.2 - PS-6a NIST SP 800-53 R4 SA-21[S]{1} NIST SP 800-53 r5 - SA-21a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-6[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-6a PCI DSS v3.2.1 12.4
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA HITRUST De-ID Framework PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	The terms and conditions of employment reflect the organization's security policy. Terms and conditions of employment: clarify and state that all employees, contractors, and third-party users who are given access to covered information sign a confidentiality or non-disclosure agreement prior to being given access to information assets; clarify and state the employee's, contractor's, and any other user's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation); clarify and state responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor, or third-party user; clarify and state responsibilities of the employee, contractor, or third-party user for the handling of information received from other companies or external parties; clarify and state responsibilities of the organization for the handling of covered information, including covered information created as a result of, or in the course of, employment with the organization; clarify and state responsibilities that are extended outside the organization's premises and outside normal working hours (e.g., in the case of home-working); clarify and state actions to be taken if the employee, contractor, or third-party user disregards the organization's security requirements; and ensure that conditions relating to security policy survive the completion of the employment in perpetuity. The organization maintains a list of all authorized signed non-disclosure agreement (NDA) forms. This list is kept up to date to reflect personnel or other workforce member changes and departures.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC1.4 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HITRUST De-ID Framework - De-ID Framework v1 Non-disclosure and Confidentiality: Policy IRS Pub 1075 - PS-6(3)b IRS Pub 1075 - SR-3(3) ISO/IEC 27002:2022 - 6(6) ISO/IEC 27799:2016 7.1.2 NIST Cybersecurity Framework v1.1 - ID.GV-3 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST SP 800-53 R4 PS-4(1)b[S]{1} NIST SP 800-53 R4 PS-6(3)b[S]{0} NIST SP 800-53 R4 PS-6a[HML]{1} NIST SP 800-53 R4 PS-6c[HML]{1} NIST SP 800-53 r5 - PS-3(1) NIST SP 800-53 r5 - PS-4(1)b NIST SP 800-53 r5 - PS-6(3)a NIST SP 800-53 r5 - PS-6(3)b NIST SP 800-53 r5 - PS-6a NIST SP 800-53 r5 - PS-6c1 PCI DSS v3.2.1 12.4
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every 365 days, whichever occurs first. The organization ensures that individuals requiring access to organizational information or information systems sign appropriate access agreements prior to being granted access and re-acknowledges such agreements when they are updated, or within 365 days, to maintain access to organizational information systems.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization reviews/updates the access agreements within every 365 days. The organization ensures that individuals requiring access to organizational information or information systems sign appropriate access agreements prior to being granted access. The organization re-acknowledges access agreements to maintain access to organizational information systems when access agreements have been updated.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization reviews information system access authorizations and initiates appropriate actions when personnel are reassigned or transferred to other positions within the organization.

Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	With respect to clinical staff, the terms and conditions of employment specify what rights of access such staff will have to the records of subjects of care, and to the associated health information systems in the event of third-party claims.

Objective Name: 02.03 During Employment

Control Objective:	To ensure that employees, contractors, and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Control Reference: 02.d Management Responsibilities

Control Specification:	Management shall require employees, and where applicable, contractors and third-party users, to apply security in accordance with established policies and procedures of the organization.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust Supplemental
Level 1 Implementation (example):	Employees, contractors, and third-party users are: properly briefed on their information security roles and responsibilities prior to being granted access to covered and/or confidential information or information systems; provided with guidelines to state security expectations of their role within the organization; motivated and comply with the security policies of the organization; achieve a level of awareness on security relevant to their roles and responsibilities within the organization; conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and continue to have the skills and qualifications appropriate to their roles and responsibilities.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.10(a)(1) 23 NYCRR 500 - 500.10(a)(2) 23 NYCRR 500 - 500.10(a)(3) 23 NYCRR 500 - 500.10(b) 23 NYCRR 500 - 500.11(a)(1) 23 NYCRR 500 - 500.11(a)(2) 23 NYCRR 500 - 500.11(a)(3) 23 NYCRR 500 - 500.11(b)(2) 23 NYCRR 500 - 500.11(b)(3) 23 NYCRR 500 - 500.11(b)(4) 23 NYCRR 500 - 500.11(c) AICPA Trust Services Criteria - AICPA 2017 CC1.4 AICPA Trust Services Criteria - AICPA 2017 CC2.2 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-15 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(i) ISO/IEC 27001:2022 - 7.3a ISO/IEC 27001:2022 - 7.3b ISO/IEC 27001:2022 - 7.4b ISO/IEC 27001:2022 - 7.4c ISO/IEC 27001:2022 - 7.4d ISO/IEC 27799:2016 7.2.1 MARS-E v2.2 - MA-1c NIST Cybersecurity Framework v1.1 - ID.AM-6 NIST Cybersecurity Framework v1.1 - PR.AT-1 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST SP 800-53 R4 PS-3(1)[S]{0} NIST SP 800-53 R4 PS-3(2)[S]{1} NIST SP 800-53 r5 - PS-3(1) NIST SP 800-53 r5 - PS-3(2) NY OHIP Moderate-Plus Security Baseline v5.0 - MP-1[PHI.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-13[IS.1c] PCI DSS v3.2.1 12.3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)? No

Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The organization has an information security workforce development and improvement program. The organization ensures plans for security testing, training, and monitoring activities are developed, maintained, and executed in a timely manner. The organization reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.2 AICPA Trust Services Criteria - AICPA 2017 CC3.2 Banking Requirements - FFIEC IS v2016 A.2.10 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-13 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-14 (HIGH; MOD) Health Industry Cybersecurity Practices - 10.S.A Health Industry Cybersecurity Practices - 2.L.B HIPAA Privacy Rule - 164.530(i)(1) HIPAA Security Rule - § 164.308(a)(2) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(D) HIPAA Security Rule - § 164.310(b) HIPAA Security Rule - § 164.312(a)(1) HIPAA Security Rule - § 164.316(b)(1)(i) IRS Pub 1075 - PM-14b IRS Pub 1075 - PM-4b ISO/IEC 27002:2022 - 5(2) ISO/IEC 27799:2016 7.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - IR-2a MARS-E v2.2 - PM-13 MARS-E v2.2 - PM-14a1 MARS-E v2.2 - PM-14a2 MARS-E v2.2 - PM-14b NIST Cybersecurity Framework v1.1 - PR.AC-3 NIST Cybersecurity Framework v1.1 - PR.AT-1 NIST Cybersecurity Framework v1.1 - PR.IP-10 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - RS.RP-1 NIST SP 800-53 R4 AC-20(3)[S]{1} NIST SP 800-53 R4 PM-14[HML]{0} NIST SP 800-53 R4 SA-17(6)[S]{0} NIST SP 800-53 r5 - PM-14 NIST SP 800-53 r5 - SA-17(6) NY OHIP Moderate-Plus Security Baseline v5.0 - PM-13 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-13[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14a1 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14a2 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14b PCI DSS v3.2.1 12.3.5 Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(c) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(g) Veterans Affairs Cybersecurity Program Directive 6500 - c(3)(d)

Level CMS Implementation Requirements

Level CMS Implementation (example):	The organization reviews and updates the risk management strategy at least every 365 days or as required, to address organizational changes.

Level DGF Implementation Requirements	
Level DGF Implementation (example):	Operational processes for Data Governance have been implemented and integrated into work. Data Custodians ensure that the strategic vision for Data Governance satisfies short-term, mid-term, and long-term needs of the custodian's domain/application/business segment, as applicable.

Control Reference: 02.e Information Security Awareness, Education, and Training	
Control Specification:	All employees of the organization, and contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP FISMA Banking Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 1 Implementation (example):	The organization provides role-based security-related training, especially for personnel with significant security responsibilities (e.g., system administrators), prior to accessing the organization's information resources, when required by system or environment changes, when entering into a new position that requires additional role-specific training, and no less than annually thereafter. The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, prior to accessing any system's information.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.14(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-16 (HIGH) FedRAMP - AT-3a[H] FedRAMP - AT-3a[L] FedRAMP - AT-3a[M] FedRAMP - AT-3b[H] FedRAMP - AT-3b[L] FedRAMP - AT-3b[M] FedRAMP - AT-3c[H] FedRAMP - AT-3c[L] FedRAMP - AT-3c[M] Health Industry Cybersecurity Practices - 1.M.D Health Industry Cybersecurity Practices - 1.S.B Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 4.S.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Privacy Rule - 164.530(b)(2)(i)(A) HIPAA Privacy Rule - 164.530(b)(2)(i)(B) HIPAA Privacy Rule - 164.530(b)(2)(i)(C) HIPAA Privacy Rule - 164.530(b)(2)(ii) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(5)(ii)(A) IRS Pub 1075 - 2.D.2.1(9) ISO/IEC 27002:2022 - 6(3) MARS-E v2.2 - AT-3a MARS-E v2.2 - AT-3b MARS-E v2.2 - AT-3c NIST Cybersecurity Framework v1.1 - PR.AT-2 NIST Cybersecurity Framework v1.1 - PR.AT-5 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST SP 800-171 r2 - 3.2.1[a] NIST SP 800-171 r2 - 3.2.1[b] NIST SP 800-171 r2 - 3.2.1[c] NIST SP 800-171 r2 - 3.2.1[d] NIST SP 800-171 r2 - 3.2.2[a] NIST SP 800-171 r2 - 3.2.2[b] NIST SP 800-171 r2 - 3.2.2[c] NIST SP 800-53 R4 AT-3[HML]{0} NIST SP 800-53 R4 SA-19(1)[S]{0} NIST SP 800-53 r5 - AT-3a NIST SP 800-53 r5 - SR-11(1) NY OHIP Moderate-Plus Security Baseline v5.0 - AT-2b NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3(5) NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3(5)[IS.4] NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3(5)[IS.5] NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3a2 Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(d) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(e)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)? No
Level 2 Regulatory Factors:	DirectTrust EHNAC FTC Red Flags Rule (16 CFR 681) 23 NYCRR 500 CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act High Low Moderate Supplemental
Level 2 Implementation (example):	Security awareness training commences with a formal induction process designed to introduce the organization's security and privacy policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee is hired. Ongoing training includes security requirements, privacy requirements, training in the correct use of information assets and facilities, and discusses how the organization addresses each area of the HITRUST CSF (e.g., audit logging and monitoring), how events or incidents are identified (e.g., monitoring for inappropriate or failed user logins), and the actions the organization takes in response to events or incidents (e.g., notifying the workforce member or the members supervisor), as appropriate to the area of training. The organization provides incident response and contingency training to information systems users consistent with assigned roles and responsibilities within 90 days of assuming an incident response role or responsibility, when required by information system changes, and within every 365 days thereafter.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.1 AICPA Trust Services Criteria - AICPA 2017 CC1.4 AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC2.3 Banking Requirements - FFIEC IS v2016 A.6.8(f) CIS Controls v7.1 - CIS CSC v7.1 17.3 CIS Controls v7.1 - CIS CSC v7.1 18.6 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-02(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-03(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-04 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-4 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-14 (HIGH; MOD) FedRAMP - AT-4a[H] FedRAMP - AT-4a[L] FedRAMP - AT-4a[M] FedRAMP - IR-8e[H] FedRAMP - IR-8e[L] FedRAMP - IR-8e[M] FTC Red Flags Rule (16 CFR 681) - 681.1e3 HIPAA Privacy Rule - 164.530(b)(1) HIPAA Privacy Rule - 164.530(b)(2)(i)(A) HIPAA Privacy Rule - 164.530(b)(2)(i)(B) HIPAA Privacy Rule - 164.530(b)(2)(i)(C) HIPAA Privacy Rule - 164.530(b)(2)(ii) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(5)(ii)(A) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HITRUST De-ID Framework - De-ID Framework v1 Privacy and Security Training: General HITRUST De-ID Framework - De-ID Framework v1 Storage (Minimal Locations Authorized): Implementation IRS Pub 1075 - 2.B.7.3(3) IRS Pub 1075 - AT-2b IRS Pub 1075 - AT-2c ISO/IEC 27799:2016 7.2.2 MARS-E v2.2 - AT-2(2)a MARS-E v2.2 - AT-2(2)b MARS-E v2.2 - AT-2(2)c MARS-E v2.2 - AT-2(2)d MARS-E v2.2 - CP-3a MARS-E v2.2 - CP-3b MARS-E v2.2 - CP-3c MARS-E v2.2 - PM-12 NIST Cybersecurity Framework v1.1 - PR.AT-1 NIST Cybersecurity Framework v1.1 - PR.AT-4 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST Cybersecurity Framework v1.1 - RS.CO-1

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 R4 AT-2(2)[HM]{0} NIST SP 800-53 R4 AT-2[HML]{0} NIST SP 800-53 R4 AT-3(3)[S]{1} NIST SP 800-53 R4 AT-4a[HML]{0} NIST SP 800-53 R4 CP-3[HML]{0} NIST SP 800-53 R4 IR-2[HML]{0} NIST SP 800-53 R4 IR-8e[HML]{0} NIST SP 800-53 R4 PL-4b[HML]{1} NIST SP 800-53 R4 PM-13[HML]{0} NIST SP 800-53 r5 - AT-2(2) NIST SP 800-53 r5 - AT-2(3) NIST SP 800-53 r5 - AT-2(5) NIST SP 800-53 r5 - AT-2(6) NIST SP 800-53 r5 - AT-2a1 NIST SP 800-53 r5 - AT-2a2 NIST SP 800-53 r5 - AT-2b NIST SP 800-53 r5 - AT-2c NIST SP 800-53 r5 - AT-2d NIST SP 800-53 r5 - AT-3(3) NIST SP 800-53 r5 - AT-3b NIST SP 800-53 r5 - AT-3c NIST SP 800-53 r5 - AT-4a NIST SP 800-53 r5 - CP-3 NIST SP 800-53 r5 - IR-2 NIST SP 800-53 r5 - IR-8d NIST SP 800-53 r5 - PL-4b NIST SP 800-53 r5 - PM-13 NIST SP 800-53 r5 - PS-3(1) NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3a1 NY OHIP Moderate-Plus Security Baseline v5.0 - CP-3a NY OHIP Moderate-Plus Security Baseline v5.0 - CP-3b NY OHIP Moderate-Plus Security Baseline v5.0 - CP-3c PCI DSS v3.2.1 12.6 PCI DSS v3.2.1 12.6.1 PCI DSS v3.2.1 12.6.2 PCI DSS v3.2.1 6.5 PCI DSS v3.2.1 9.9 PCI DSS v3.2.1 9.9.3 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(8) Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(d) Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(e)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	

Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate
Level 3 Implementation (example):	The organization maintains a documented list of each individual who completes the on-boarding process and ensures that training records are retained for at least five years. The organization trains workforce members on how to properly respond to perimeter security alarms.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-04 (HIGH; MOD) FedRAMP - AT-4b[H] FedRAMP - AT-4b[L] FedRAMP - AT-4b[M] HIPAA Security Rule - § 164.308(a)(5)(i) HITRUST De-ID Framework - De-ID Framework v1 Perimeter Security (Alarms): Testing IRS Pub 1075 - AT-4b MARS-E v2.2 - AT-4b MARS-E v2.2 - AT-4c NIST SP 800-53 R4 AT-4b[HML]{0} NIST SP 800-53 r5 - AT-4b NY OHIP Moderate-Plus Security Baseline v5.0 - AT-4[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - AT-4c
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization: performs a gap analysis to assess skills employees need and which behaviors employees are not adhering to; builds a baseline training and awareness roadmap for all employees; and delivers additional awareness and training content to fill the skills gap through an awareness and training program.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations and employs automated mechanisms to provide a more thorough and realistic training environment. The organization requires the developer of the information system, system component, or information system service to provide appropriate training (or training materials), for affected personnel, on the correct use and operation of the implemented security functions, controls, and/or mechanisms.
Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	Awareness training includes training on the organization’s breach reporting policies and procedures.
Level Federal Implementation Requirements	
Level Federal Implementation (example):	The organization has implemented an Operations Security (OPSEC) program.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization provides contingency training to information system users consistent with assigned roles and responsibilities within 10 days of assuming an incident response role or responsibility, when required by information system changes, and within every 365 days thereafter. The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by information system changes, and on an annual basis.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization provides awareness training on protecting FTI, on disclosing FTI, on how FTI security requirements are communicated to end users, on the (possible) sanctions for misuse of FTI, initially prior to granting access to FTI, and annually thereafter. Training is user specific to ensure that all personnel receive appropriate training for a particular job, such as training required for administrators or auditors. The organization provides refresher training on incident response policies and procedures prior to granting access to FTI and annually.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization ensures the importance of the cardholder data security policy and procedures and is included in a formal security awareness program for all personnel, and trains personnel to be aware of attempted tampering or replacement of devices. Organizational training includes: verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices; not installing, replacing, or returning devices without verification; being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices); and reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
Level Title 21 CFR Part 11 Implementation Requirements	
Level Title 21 CFR Part 11 Implementation (example):	Persons who develop, maintain, or use electronic record/electronic signature systems have the proper and sufficient education, training, and experience to perform their assigned tasks.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: within one month of assuming an incident response role or responsibility; when required by information system changes; and within every 365 days thereafter. The organization develops an information security and privacy education and awareness training program that is implemented for all employees and individuals working on behalf of CMS who access, use, manage, or develop information systems.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	Individuals are adequately trained on the Data Governance framework, policies, and related implementation expectations.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization develops, documents, and disseminates to organization-defined personnel or roles a security awareness and privacy training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the security awareness and privacy training policy and associated security awareness and training controls. The organization ensures the security awareness and privacy training policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. The organization designates an organization-defined official to manage the development, documentation, and dissemination of the security and privacy awareness and training policy and procedures. The organization reviews and updates the current awareness and training policy at least annually or whenever a significant change occurs, and awareness and training procedures at least annually or whenever a significant change occurs.

Control Reference: 02.f Disciplinary Process

Control Specification:	There shall be a formal disciplinary process for employees who have violated security policies and procedures.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA HITRUST De-ID Framework State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization’s formal sanctions process: includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action; identifies the individual sanctioned; and identifies the reason for the sanction. The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. The organization notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(B)(xviii)(I) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(B)(xviii)(II) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(B)(xviii)(III) AICPA Trust Services Criteria - AICPA 2017 CC1.1 AICPA Trust Services Criteria - AICPA 2017 CC1.5 AICPA Trust Services Criteria - AICPA 2017 CC5.3 AICPA Trust Services Criteria - AICPA 2017 CC7.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-08 (HIGH; MOD) FedRAMP - PS-8a[H] FedRAMP - PS-8a[L] FedRAMP - PS-8a[M] FedRAMP - PS-8b[L] FedRAMP - PS-8b[M] HIPAA Privacy Rule - 164.530(e)(1) HIPAA Privacy Rule - 164.530(e)(2) HIPAA Security Rule - § 164.308(a)(1)(ii)(C) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Sanctions: General ISO/IEC 27002:2022 - 6(4) MARS-E v2.2 - PS-8a MARS-E v2.2 - PS-8b NIST SP 800-53 R4 PS-8[HML]{0} NIST SP 800-53 r5 - PS-8a NIST SP 800-53 r5 - PS-8b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-8[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-8a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-8b State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(d) Veterans Affairs Cybersecurity Program Directive 6500 - a(3)(b)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No
Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA HITRUST De-ID Framework State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)

Level 2 Implementation (example):	Sanctions for violations of the organizations security policies do not commence without prior verification of a breach. The formal disciplinary process ensures that correct and fair treatment for employees who are suspected of committing breaches of security, and graduated response that takes into consideration factors (impact, number of offenses, training, regulatory requirements, and contractual obligations). For each incident, the organization documents personnel involved in the disciplinary process, the steps taken, timeline associated with the steps taken, the steps taken for notification, the rationale for the discipline, whether the discipline was due to a compliance failure, and the final outcome. The organization maintains a list of employees involved in security incident investigations, and the resulting outcome.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(j) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-08 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-08 (HIGH; MOD) HIPAA Privacy Rule - 164.530(e)(1) HIPAA Privacy Rule - 164.530(e)(2) HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(C) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HITRUST ISO/IEC 27799:2016 7.2.3 OCR Audit Protocol (2016) 164.308(a)(1)(ii)(C) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(d)
Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	The organization’s formal sanctions process includes failure to comply with established privacy policies and procedures.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization notifies at a minimum, the ISSO and/or similar role within the organization within organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization must notify designated personnel within 72 hours when a formal employee sanction process is initiated, identifying the individual sanctioned and any required administrative actions. The organization employs a formal sanctions process for personnel failing to comply with established information security and privacy policies and procedures.

Objective Name: 02.04 Termination or Change of Employment

Control Objective:	To ensure that the access rights are properly removed and that assets are recovered for employees and contractors who have been terminated or transferred.

Control Reference: 02.g Termination or Change Responsibilities

Control Specification:	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP
Level 1 Implementation (example):	The organization has a documented termination checklist that identifies all the steps to be taken and assets to be collected.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04 (HIGH; MOD) Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(3)(ii)(C) HITRUST IRS Pub 1075 - 2.C.4.3(2)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA CA Civil Code § 1798.81.5 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	The organization terminates access when the access is no longer needed, assigns of responsibility for removing information system and/or physical access, and timely communicates termination actions to ensure that the termination procedures are appropriately followed. The organization has a documented termination process for all employees and other workforce members. The organization has a formal termination process that ensures exit interviews address organization-defined information and security items, all organization information system related property and access is retrieved and revoked, knowledge and information is transferred, and appropriate personnel are provided with access to official records created by a terminated employee or when the arrangement of a workforce member ends.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.4 Banking Requirements - FFIEC IS v2016 A.6.8(c) CIS Controls v7.1 - CIS CSC v7.1 16.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-05 (HIGH; MOD) FedRAMP - PS-4c[H] FedRAMP - PS-4c[L] FedRAMP - PS-4c[M] FedRAMP - PS-4d[H] FedRAMP - PS-4d[L] FedRAMP - PS-4d[M] FedRAMP - PS-4e[H] FedRAMP - PS-4e[L] FedRAMP - PS-4e[M] Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 3.S.A HIPAA Security Rule - § 164.308(a)(3)(ii)(C) HITRUST IRS Pub 1075 - 2.C.4.3(1) IRS Pub 1075 - 2.C.4.3(3) IRS Pub 1075 - PS-4c IRS Pub 1075 - PS-4e IRS Pub 1075 - PS-6(3)a ISO/IEC 27002:2022 - 6(5) ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 7.3.1 ISO/IEC 27799:2016 9.2.6 MARS-E v2.2 - PS-4c MARS-E v2.2 - PS-4d MARS-E v2.2 - PS-4e NIST SP 800-53 R4 PS-4(1)a[S]{0} NIST SP 800-53 R4 PS-4a[HML]{1} NIST SP 800-53 R4 PS-4c[HML]{0} NIST SP 800-53 R4 PS-4d[HML]{0} NIST SP 800-53 R4 PS-4e[HML]{0} NIST SP 800-53 r5 - PS-4(1)a NIST SP 800-53 r5 - PS-4a NIST SP 800-53 r5 - PS-4c NIST SP 800-53 r5 - PS-4d NIST SP 800-53 r5 - PS-4e NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4c NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4d NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4e

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP CMS Minimum Security Requirements (High) High
Level 3 Implementation (example):	The organization employs automated mechanisms to notify specific personnel or roles (formally defined by the organization) upon termination of an individual.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04(02) (HIGH) FedRAMP - PS-4 (2)[H] HIPAA Security Rule - § 164.308(a)(3)(ii)(C) NIST SP 800-53 R4 PS-4(2)[H]{0} NIST SP 800-53 r5 - AC-2h NIST SP 800-53 r5 - PS-4(2) NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4(2) NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4f
Level CMS Implementation Requirements	
Level CMS Implementation (example):	All access and privileges to CMS systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence). When personnel are transferred or reassigned, the organization: reissues appropriate information system-related property (e.g., keys, identification cards, building passes); notifies security management; closes obsolete accounts; establishes new accounts, as necessary; and notifies defined personnel or roles (defined in the applicable security plan) within one business day.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization notifies defined personnel or roles within five business days of when personnel are transferred or reassigned.

Control Reference: 02.h Return of Assets

Control Specification:	All employees, contractors, and third-party users shall return all of the organization's assets in their possession upon termination of their employment, contract, or agreement.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The termination process includes the return of all previously issued software in the termination process, all corporate documents in the termination process, all equipment in the termination process, and all other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media in the termination process.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04 (HIGH; MOD) Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(3)(ii)(C) IRS Pub 1075 - PS-4d ISO/IEC 27002:2022 - 5(11) ISO/IEC 27799:2016 8.1.4 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(e)

Control Reference: 02.i Removal of Access Rights

Control Specification:	The access rights of all employees, contractors, and third-party users to information and information assets shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment (i.e., upon transfer within the organization).
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust CA Civil Code § 1798.81.5 Texas Medical Records Privacy Act High Low Moderate
Level 1 Implementation (example):	The organization ensures logical and physical access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in responsibility, or employment.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.07 AICPA Trust Services Criteria - AICPA 2017 CC6.4 Banking Requirements - FFIEC IS v2016 A.6.8(c) CIS Controls v7.1 - CIS CSC v7.1 16.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-05 (HIGH; MOD) Health Industry Cybersecurity Practices - 3.M.B Health Industry Cybersecurity Practices - 3.S.A Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(3)(ii)(C) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - 2.D.6(2) IRS Pub 1075 - PS-4e ISO/IEC 27799:2016 9.2.6 NIST Cybersecurity Framework v1.1 - PR.AC-2 NIST SP 800-171 r2 - 3.9.2[a] NIST SP 800-171 r2 - 3.9.2[b] NIST SP 800-171 r2 - 3.9.2[c] NIST SP 800-53 R4 PS-4b[HML]{0} NIST SP 800-53 r5 - PS-4b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-5[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-5a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-5c

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	When an employee or other workforce member moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but no longer than 30 days. The organization also ensures employees or workforce members that are terminated understand their obligations to ensure any covered information for which they had prior access remains confidential (e.g., during an exit interview). Access rights to information assets and facilities are reduced or removed before the employment or other workforce arrangement terminates or changes depending on the evaluation of risk factors. The risk factors evaluated when reducing or removing access rights upon termination or change in work arrangement includes: whether the termination or change is initiated by the employee, contractor, third-party user, other workforce member, or by management; the reason of termination; current responsibilities of the employee, contractor, workforce member or any other user; and the value of the assets currently accessible.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.8(c) CIS Controls v7.1 - CIS CSC v7.1 16.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-05 (HIGH; MOD) Health Industry Cybersecurity Practices - 3.M.B HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(3)(ii)(C) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) IRS Pub 1075 - 2.C.4.3(1) IRS Pub 1075 - 2.C.4.3(2) ISO/IEC 27799:2016 9.2.6 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PS-4a MARS-E v2.2 - PS-4g MARS-E v2.2 - PS-5b4 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST SP 800-53 R4 PS-4(1)b[S]{2} NIST SP 800-53 R4 PS-4a[HML]{2} NIST SP 800-53 R4 PS-5a[HML]{0} NIST SP 800-53 R4 PS-5b[HML]{0} NIST SP 800-53 R4 PS-5c[HML]{0} NIST SP 800-53 r5 - PS-4(1)b NIST SP 800-53 r5 - PS-4a NIST SP 800-53 r5 - PS-5a NIST SP 800-53 r5 - PS-5b NIST SP 800-53 r5 - PS-5c NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2l NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-4g NY OHIP Moderate-Plus Security Baseline v5.0 - PS-5b1 NY OHIP Moderate-Plus Security Baseline v5.0 - PS-5b4 PCI DSS v3.2.1 8.1.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	FISMA PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate

Level 3 Implementation (example):	Upon termination, the access rights for the terminated individuals are disabled in a timely manner, at least within 24 hours. Changes of employment or other workforce arrangement (e.g., transfers) are reflected in removal of all access rights that were not approved for the new employment or workforce arrangement. Access changes due to personnel transfer are managed effectively. Old accounts are closed after 90 days, and new accounts opened. The access rights removed or adapted include: physical access; logical access; keys; identification cards; IT systems access; applications access; subscriptions; and removal from any documentation that identifies them as a current member of the organization. If a departing employee, contractor, third-party user, or other workforce member has known passwords for accounts remaining active, these are changed upon termination or change of employment, contract, agreement, or other workforce arrangement.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-2 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-05 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) IRS Pub 1075 - 2.B.3.4(2) IRS Pub 1075 - PS-4a IRS Pub 1075 - PS-4b ISO/IEC 27799:2016 9.2.6 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST SP 800-53 R4 PE-3g[HML]{1} NIST SP 800-53 r5 - PE-3g PCI DSS v3.2.1 8.1.3 Supplemental Requirements - SR v6.4 19b-0
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization, upon termination of individual employment, disables information system access within eight hours and terminates/revokes any authenticators/credentials associated with the individual.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Accounts are disabled within 120 days when they have expired, are no longer associated to a user or individual, are in violation of organizational policy, or have been inactive for 120 days for non-privileged accounts and 60 days for privileged accounts.
Level Providers Implementation Requirements	
Level Providers Implementation (example):	Any organization that processes protected health information will terminate related user access privileges for any departing permanent employee, permanent temporary employee, third-party contractor, volunteer.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	Upon termination resulting from, or resignation during, an investigation into the actual or suspected inappropriate collection, use, disclosure, retention or disposal of PHI, access rights for the terminated individual are disabled in a timely manner and written notice of the termination is provided within 30 days to relevant external points of contact (e.g., to the colleges or boards of health that the individual is a member of).

Control Category: 03.0 - Risk Management

Objective Name: 03.01 Risk Management Program

Control Objective:	To develop and implement a Risk Management Program that addresses Risk Assessments, Risk Mitigation, and Risk Evaluations.

Control Reference: 03.a Risk Management Program Development

Control Specification:	Organizations shall develop and maintain a risk management program to manage risk to an acceptable level.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC 15 390.2 - 1 TAC § 390.2(b) 23 NYCRR 500 - 500.05(a) 23 NYCRR 500 - 500.05(b) 23 NYCRR 500 - 500.09(a) 23 NYCRR 500 - 500.09(b)(1) 23 NYCRR 500 - 500.09(b)(2) 23 NYCRR 500 - 500.09(b)(3) AICPA Trust Services Criteria - AICPA 2017 CC3.3 Banking Requirements - FFIEC IS v2016 A.2.11 Banking Requirements - FFIEC IS v2016 A.3.1 Banking Requirements - FFIEC IS v2016 A.6.4(a) Banking Requirements - FFIEC IS v2016 A.7.1 Banking Requirements - FFIEC IS v2016 A.7.2 Banking Requirements - FFIEC IS v2016 A.7.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-03 (HIGH; MOD) EU GDPR Article 32(2) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) IRS Pub 1075 - PM-9b ISO 31000:2018 - 5.2 ISO 31000:2018 - 5.3 ISO 31000:2018 - 5.4.2 ISO 31000:2018 - 5.6 ISO 31000:2018 - 6.1 ISO 31000:2018 - 6.2 ISO 31000:2018 - 6.6 ISO/IEC 27001:2022 - 6.1.1d ISO/IEC 27001:2022 - 6.1.1e1 ISO/IEC 27001:2022 - 6.1.1e2 ISO/IEC 27001:2022 - 6.1.2a1 ISO/IEC 27001:2022 - 6.1.2c1 ISO/IEC 27001:2022 - 6.1.2d3 ISO/IEC 27001:2022 - 6.1.2e1 ISO/IEC 27001:2022 - 6.1.2e2 ISO/IEC 27001:2022 - 6.2c ISO/IEC 27001:2022 - 8.1a MARS-E v2.2 - PM-11a MARS-E v2.2 - PM-11b MARS-E v2.2 - PM-9a NIST AI RMF 1.0 - GOVERN 1.2 NIST AI RMF 1.0 - GOVERN 1.4 NIST AI RMF 1.0 - GOVERN 1.5 NIST AI RMF 1.0 - GOVERN 2.1 NIST AI RMF 1.0 - GOVERN 2.3 NIST AI RMF 1.0 - GOVERN 3.2 NIST AI RMF 1.0 - MANAGE 1.1 NIST AI RMF 1.0 - MANAGE 3.2 NIST AI RMF 1.0 - MANAGE 4.1 NIST AI RMF 1.0 - MAP 5.2 NIST AI RMF 1.0 - MEASURE 2.2 NIST AI RMF 1.0 - MEASURE 2.4 NIST AI RMF 1.0 - MEASURE 2.8 NIST AI RMF 1.0 - MEASURE 3.3 NIST Cybersecurity Framework v1.1 - ID.RA-5 NIST Cybersecurity Framework v1.1 - ID.RM-1

Level 1 Authoritative Source Mapping (Cont.):	NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST SP 800-53 R4 PM-9a[HML]{0} NIST SP 800-53 R4 PM-9c[HML]{0} NIST SP 800-53 r5 - PM-28 NIST SP 800-53 r5 - PM-9a1 NIST SP 800-53 r5 - PM-9c NY OHIP Moderate-Plus Security Baseline v5.0 - CA-7[PRIV.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-11a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-11c NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28a1 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28a2 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28a3 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28a4 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9a1 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9b NY OHIP Moderate-Plus Security Baseline v5.0 - RA-7 NY OHIP Moderate-Plus Security Baseline v5.0 - RA-7[IS.1] Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(b) Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(h) Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(a) Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(b) Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(c) Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(d) Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(h)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework Banking Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	The organization evaluates, and manages risk prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.

	A formal risk assessment is performed. Risk treatment processes are implemented. A repository and tracking system for risk assessments performed is implemented. Risk mitigation is completed or underway.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC 15 390.2 - 1 TAC § 390.2(b) Banking Requirements - FFIEC IS v2016 A.2.11 Banking Requirements - FFIEC IS v2016 A.3.1 Banking Requirements - FFIEC IS v2016 A.7.1 Banking Requirements - FFIEC IS v2016 A.7.2 Banking Requirements - FFIEC IS v2016 A.7.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-03 (HIGH; MOD) ISO 31000:2018 - 6.4.4 ISO/IEC 27001:2022 - 6.1.2f ISO/IEC 27001:2022 - 6.1.3g ISO/IEC 27001:2022 - 8.3a NIST AI RMF 1.0 - GOVERN 1.4 NIST AI RMF 1.0 - MANAGE 1.1 NIST AI RMF 1.0 - MANAGE 1.3 NIST Cybersecurity Framework v1.1 - ID.GV-4 NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST SP 800-53 R4 PM-9b[HML]{0} NIST SP 800-53 r5 - PM-9b Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(b) Veterans Affairs Cybersecurity Program Directive 6500 - d(4)(c)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FTC Red Flags Rule (16 CFR 681) Texas Medical Records Privacy Act
Level 3 Implementation (example):	The organization develops, and implements a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account that involves or is designed to permit multiple payments or transactions. The organization defines and incorporates existing policies and implement procedures to: identify relevant patterns, practices, or specific activities that indicate the possible existence of identity theft for the accounts, and incorporate those patterns, practices, and activities into its program; detect patterns, practices, and activities that have been incorporated into the program; respond appropriately to any patterns, practices, and activities that are detected to prevent and mitigate identity theft; and ensure the program and patterns, practices, and activities are updated at least annually, to reflect changes in risks to customers and to the safety and soundness of the organization.

	The organization has identified that 'Personal Identifying Information' or 'Personally Identifiable Information' (PII) means information that alone, or in conjunction with other information, identifies an individual. The organization's definition of PII includes: name, social security number, date of birth, or government-issued identification number; mother's maiden name; unique biometric data, including the individuals fingerprint, voice print, and retina or iris image; electronic identification number, address, or routing code; and telecommunication access device.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) FTC Red Flags Rule (16 CFR 681) - 681.1d1 FTC Red Flags Rule (16 CFR 681) - 681.1d2.i FTC Red Flags Rule (16 CFR 681) - 681.1d2.ii FTC Red Flags Rule (16 CFR 681) - 681.1d2.iii FTC Red Flags Rule (16 CFR 681) - 681.1d2.iv FTC Red Flags Rule (16 CFR 681) - 681.A1 FTC Red Flags Rule (16 CFR 681) - 681.A2.a1 FTC Red Flags Rule (16 CFR 681) - 681.A2.a2 FTC Red Flags Rule (16 CFR 681) - 681.A2.a3 FTC Red Flags Rule (16 CFR 681) - 681.A2.a4 FTC Red Flags Rule (16 CFR 681) - 681.A2.b1 FTC Red Flags Rule (16 CFR 681) - 681.A2.b2 FTC Red Flags Rule (16 CFR 681) - 681.A2.b3 FTC Red Flags Rule (16 CFR 681) - 681.A3.a FTC Red Flags Rule (16 CFR 681) - 681.A3.b FTC Red Flags Rule (16 CFR 681) - 681.A4.a FTC Red Flags Rule (16 CFR 681) - 681.A4.b FTC Red Flags Rule (16 CFR 681) - 681.A4.c FTC Red Flags Rule (16 CFR 681) - 681.A4.d FTC Red Flags Rule (16 CFR 681) - 681.A4.e FTC Red Flags Rule (16 CFR 681) - 681.A4.f FTC Red Flags Rule (16 CFR 681) - 681.A4.g FTC Red Flags Rule (16 CFR 681) - 681.A4.h FTC Red Flags Rule (16 CFR 681) - 681.A4.i FTC Red Flags Rule (16 CFR 681) - 681.A5.a FTC Red Flags Rule (16 CFR 681) - 681.A5.b FTC Red Flags Rule (16 CFR 681) - 681.A5.c FTC Red Flags Rule (16 CFR 681) - 681.A5.d FTC Red Flags Rule (16 CFR 681) - 681.A5.e FTC Red Flags Rule (16 CFR 681) - 681.A6.a2 FTC Red Flags Rule (16 CFR 681) - 681.A6.a3 NIST Cybersecurity Framework v1.1 - DE.DP-5 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST Cybersecurity Framework v1.1 - RS.RP-1
Level Cloud Service Providers Implementation Requirements	
Level Cloud Service Providers Implementation (example):	Cloud service providers review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization: confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; collects PII directly from the individual to the greatest extent practicable; checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems no less often than once every 365 days; and issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

	The organization: establishes, maintains, and updates within every 365 days, an inventory of all programs and systems used for collecting, creating, using, disclosing, maintaining, or sharing Personally Identifiable Information (PII); and provides each update of the PII inventory to the organization's designated privacy official or information security official to support the establishment of information security requirements for all new or modified information systems containing PII.
Level De-ID Data Environment Implementation Requirements	
Level De-ID Data Environment Implementation (example):	The organization documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII). The organization conducts privacy impact assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	The organization maintains a general analysis of most likely scenarios for breaches of PHI security.
Level Federal Implementation Requirements	
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The organization applies security controls and privacy controls to all personal data, which includes but is not limited to PII.
Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation (example):	The licensee identifies reasonably foreseeable threats, assesses the likelihood and possible damage from such threats, assesses its policies, procedures, and systems to manage threats, and implements safeguards to manage identified threats.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization: confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; collects PII directly from the individual to the greatest extent practicable; checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems within organization-defined frequency; and issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. The organization: identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings within organization-defined frequency, at least annually, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
Level ISO/IEC 23894 Implementation Requirements	
Level ISO/IEC 23894 Implementation (example):	The organization develops, documents, and disseminates policies and statements related to AI risks and risk management to stakeholders.

	The organization issues statements related to its commitment to AI risk management to increase confidence of their stakeholders on their use of AI.

Level ISO 31000 Implementation Requirements	
Level ISO 31000 Implementation (example):	The organization evaluates its existing risk management practices and processes, evaluates any gaps, and addresses those gaps within an organization-chosen risk management framework on an annual basis. The characteristics of the chosen risk management framework (e.g., industry-accepted, regulatory-required) and the way in which they work together are customized and implemented to meet the needs of the organization. The organization implements a risk management framework (e.g., industry-accepted, regulatory-required) by developing an appropriate risk management plan including time and resources, identifying where, when, and how different types of risk management decisions are made across the organization, and by whom, modifying the applicable risk management decision-making processes where necessary, ensuring that the organization's arrangements for managing risk are clearly understood and practiced, and reviewing and updating the risk management plan at least annually for changes in the organization's risk profile and for updates to the risk management framework.

Control Reference: 03.b Performing Risk Assessments

Control Specification:	Risk Assessments shall be performed to identify and quantify risks.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust HITRUST De-ID Framework State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act High Low Moderate
Level 1 Implementation (example):	The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals and when major changes occur in the environment, and the results reviewed annually.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 23 NYCRR 500 - 500.02(b)(1) 23 NYCRR 500 - 500.03(m) 23 NYCRR 500 - 500.09(a) AICPA Trust Services Criteria - AICPA 2017 CC4.1 Banking Requirements - FFIEC IS v2016 A.4.1 Banking Requirements - FFIEC IS v2016 A.6.28(c) Banking Requirements - FFIEC IS v2016 A.6.4(a) Banking Requirements - FFIEC IS v2016 A.7.1 Banking Requirements - FFIEC IS v2016 A.7.2 Banking Requirements - FFIEC IS v2016 A.7.3 Banking Requirements - FFIEC IS v2016 A.7.4(e) Banking Requirements - FFIEC IS v2016 A.8.1(i) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-03 (HIGH; MOD) FTC Red Flags Rule (16 CFR 681) - 681.A2.b3 HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Risk Assessments: Assessments ISO 31000:2018 - 6.4.1 ISO/IEC 27799:2016 12.6.1 ISO/IEC 27799:2016 17.1.1 NIST AI RMF 1.0 - GOVERN 1.7 NIST AI RMF 1.0 - MANAGE 4.1 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST SP 800-171 r2 - 3.11.1[a] NIST SP 800-171 r2 - 3.11.1[b] NIST SP 800-53 R4 RA-3a[HML]{0} NIST SP 800-53 R4 RA-3c[HML]{0} NIST SP 800-53 r5 - RA-3d PCI DSS v3.2.1 12.2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(b)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate

Level 2 Implementation (example):	A formal, documented process is in place for identifying risks and performing risk assessments. The formal, documented process is in place for identifying risks and performing risk assessments includes: the criteria for the evaluation; the categorization of risks; communicating the results of the risk assessments to the affected parties, and to management. The organization: updates the results of a comprehensive risk assessment every two years; updates the results of a comprehensive risk assessment whenever there is a significant change to the information system or operational environment; assesses a subset of the security controls within every 365 days during continuous monitoring; reviews the risk assessment results annually. Information security risk assessments require knowledge of: external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously; the types of accounts offered by the organization and the methods the organization provides to open and access its accounts; incident histories and actual case impact scenarios; systems architectures.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.09(b)(1) AICPA Trust Services Criteria - AICPA 2017 CC3.4 Banking Requirements - FFIEC IS v2016 A.4.1 Banking Requirements - FFIEC IS v2016 A.7.1 Banking Requirements - FFIEC IS v2016 A.7.2 Banking Requirements - FFIEC IS v2016 A.7.3 Banking Requirements - FFIEC IS v2016 A.8.1(i) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-03 (HIGH; MOD) FTC Red Flags Rule (16 CFR 681) - 681.1c1 FTC Red Flags Rule (16 CFR 681) - 681.1c2 FTC Red Flags Rule (16 CFR 681) - 681.1c3 HIPAA Security Rule - § 164.308(a)(1)(ii)(A) ISO 31000:2018 - 6.4.1 ISO/IEC 27001:2022 - 6.1.2a2 ISO/IEC 27001:2022 - 6.1.2b ISO/IEC 27001:2022 - 6.1.2f NIST AI RMF 1.0 - GOVERN 1.7 NIST AI RMF 1.0 - MANAGE 4.1 NIST Cybersecurity Framework v1.1 - DE.DP-3 NIST SP 800-53 R4 CA-2b[HML]{0} NIST SP 800-53 R4 RA-3b[HML]{0} NIST SP 800-53 R4 RA-3d[HML]{0} NIST SP 800-53 R4 RA-3e[HML]{0} NIST SP 800-53 r5 - CA-2d NIST SP 800-53 r5 - RA-3c NIST SP 800-53 r5 - RA-3f NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-28b PCI DSS v3.2.1 12.2
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization assesses the security controls in the information system within every 365 days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The annual security risk assessment requirement as mandated by OMB requires all controls attributable to a system or application to be assessed over a three year period. To meet this requirement, a subset of the CMSRs is tested each year so that all security controls are tested during a three year period. The organization disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization accepts the results of an assessment of any FedRAMP Accredited 3PAO performed by any FedRAMP Accredited 3PAO when the assessment meets the conditions of the JAB/AO in the FedRAMP Repository. The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, documents risk assessment results in a security assessment report as required, reviews risk assessment results at least annually or whenever a significant change occurs, disseminates risk assessment results to organization-defined personnel or roles, and updates the risk assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation (example):	The organization implements a risk identification process that produces manageable groupings of information security threats, which include the following: a threat assessment to help focus the risk identification efforts; a method or taxonomy for categorizing threats, sources, and vulnerabilities; a process to determine the institution's information security risk profile; a validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments; and a validation though audits, self-assessments, penetration tests, and vulnerability assessments that risk decisions are informed by appropriate identification and analysis of threats and other potential causes of loss. The organization implements threat modeling (e.g., development of attack trees) as part of its risk assessment process to assist in identifying and quantifying risk in better understanding the nature, frequency, and sophistication of threats.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization conducts periodically, but at least annually, an assessment of the security and privacy controls in systems that receive, store, process or transmit FTI, including cloud environments. The organization conducts an assessment of the security and privacy controls in systems that receive, store, process, or transmit FTI immediately prior to the implementation of the cloud environment and during each annual risk assessment (or update to an existing risk assessment) thereafter. The organization ensures each aspect of a data warehouse is assessed for risk, including hardware, software, data transport, and data storage. Any risk documents identify and document all vulnerabilities, associated with a data warehousing environment.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	Prior to processing, the organization, acting as a data controller, carries out an impact assessment for personal data, taking into account the nature, scope, context, and purpose of the processing–unless a valid exception exists. The controller carries out a review to assess if processing is performed in accordance with the data impact assessment, at least when there is a change in the risk represented by processing operations.

Level HIX Implementation Requirements	
Level HIX Implementation (example):	Within every 365 days, the organization performs a documented assessment of a subset of the security and privacy controls attributable to a system or application in accordance with the Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges–such that all the controls are tested within a three year period. A security and privacy controls assessment is conducted prior to issuing the authority to operate for newly implemented, or significantly changed, systems.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	Formal risk assessments are performed at least annually and upon significant changes to the environment. The assessments will identify critical assets, identify threats, identify vulnerabilities, and result in a formal, documented analysis of risk.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	Risk assessments (analysis) used to determine whether a breach of unsecured Protected Health Information (PHI) as these terms are defined by the Secretary of Health and Human Services is reportable to the Secretary must demonstrate there is a low probability of compromise (LoProCo) rather than a significant risk of harm. The methodology, at a minimum, address the following factors: the nature of the PHI involved, including the types of identifiers involved and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; the extent to which the risk to the PHI has been mitigated; and other factors/guidance promulgated by the Secretary.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization: conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; conducts an E-Authentication Risk Assessment (ERA), as required, on systems and determines e-authentication assurance levels; documents risk assessment results in the applicable security plan; reviews risk assessment results within every 365 days; disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and updates the risk assessment before issuing a new authority to operate (ATO) package or within every three years, whichever comes first, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. For systems processing, storing, or transmitting PII (to include PHI), the organization includes an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of personally identifiable information (PII) in the related risk assessment documentation.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	A process is in place to identify key business/systems/IT organizations to have Data Governance implemented.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization analyzes the effectiveness of security solutions at least annually. The analysis of security solutions: includes the effectiveness of security controls and intended capabilities based on new and existing threat intelligence; and allows organizations to identify shortcomings in the intended security capabilities and any necessary changes to the design, architecture, and configuration of the solutions. Changes are rolled into SOP timeframes and based on criticality of the findings.

Level ISO/IEC 23894 Implementation Requirements	
Level ISO/IEC 23894 Implementation (example):	The organization aligns risk assessment activities with the system life cycle for the development and/or use of AI systems. The organization identifies assets related to the design and use of AI that fall within the scope of the risk management process, documenting considerations of both the value of the asset and the nature of the asset, both tangible (e.g. data, models, the AI system itself, the environment) and intangible (e.g., reputation, trust, individual privacy and safety).

Level ISO 31000 Implementation Requirements	
Level ISO 31000 Implementation (example):	The organization considers, documents, and communicates to decision makers potential influences and limitations to the risk analysis.

Control Reference: 03.c Risk Mitigation

Control Specification:	Risks shall be mitigated to an acceptable level.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental
Level 1 Implementation (example):	The organization implements an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC5.1 Banking Requirements - FFIEC IS v2016 A.6.4 ISO/IEC 27001:2022 - 6.1.3d ISO/IEC 27001:2022 - 8.1b NIST Cybersecurity Framework v1.1 - DE.DP-5 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST SP 800-53 R4 PL-8(1)a[S]{0} NIST SP 800-53 R4 SC-3(5)[S]{0} NIST SP 800-53 r5 - PL-8(1)a NIST SP 800-53 r5 - SC-3(5)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA Banking Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The organization has defined criteria to determine an appropriate risk treatment (e.g., accept, mitigate, transfer, or avoid) that include industry or organizational laws, regulations or standards, contractual obligations, business or other priorities, cultural fit, customer/client concerns, IT policy and strategies, risk and business strategies, cost, effectiveness, type of protection, threats covered, risk levels, existing alternatives, and additional benefits derived from the risk treatment. Further, the organization implements a process for ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained. The remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented. The organization mitigates any harmful effect that is known to the organization of a use or disclosure of covered information (e.g., PII) by the partners, vendors, contractors or similar third-party in violation of its policies and procedures.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(k) AICPA Trust Services Criteria - AICPA 2017 CC4.2 AICPA Trust Services Criteria - AICPA 2017 P6.4 AICPA Trust Services Criteria - AICPA 2017 P6.5 AICPA Trust Services Criteria - AICPA 2017 P6.6 Banking Requirements - FFIEC IS v2016 A.6.4 Banking Requirements - FFIEC IS v2016 A.6.4(a) Banking Requirements - FFIEC IS v2016 A.7.1 Banking Requirements - FFIEC IS v2016 A.7.2 Banking Requirements - FFIEC IS v2016 A.7.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-04 (HIGH; MOD) Health Industry Cybersecurity Practices - 7.L.B HIPAA Privacy Rule - 164.530(f) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.316(b)(2)(iii) IRS Pub 1075 - 2.D.9(1) ISO 31000:2018 - 6.4.4 ISO 31000:2018 - 6.5.2 ISO 31000:2018 - 6.5.3 ISO/IEC 27001:2022 - 6.1.1d ISO/IEC 27001:2022 - 6.1.3a ISO/IEC 27001:2022 - 6.1.3b ISO/IEC 27001:2022 - 6.1.3c ISO/IEC 27001:2022 - 6.1.3d ISO/IEC 27001:2022 - 6.1.3e ISO/IEC 27001:2022 - 6.1.3f ISO/IEC 27001:2022 - 6.1.3g ISO/IEC 27001:2022 - 8.3b ISO/IEC 27799:2016 12.6.1 ISO/IEC 27799:2016 12.7.1 ISO/IEC 27799:2016 17.1.1 MARS-E v2.2 - PM-4a1 MARS-E v2.2 - PM-4a2 NIST AI RMF 1.0 - GOVERN 1.4 NIST AI RMF 1.0 - GOVERN 6.2 NIST AI RMF 1.0 - MANAGE 1.1 NIST AI RMF 1.0 - MANAGE 1.2 NIST AI RMF 1.0 - MANAGE 1.3 NIST AI RMF 1.0 - MANAGE 2.4 NIST AI RMF 1.0 - MAP 3.2 NIST Cybersecurity Framework v1.1 - ID.RA-6 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST SP 800-53 R4 CA-2(3)[S]{0} NIST SP 800-53 R4 CA-5a[HML]{0} NIST SP 800-53 R4 CA-5b[HML]{0} NIST SP 800-53 R4 PM-4a[HML]{1} NIST SP 800-53 R4 PM-4b[HML]{0} NIST SP 800-53 r5 - CA-2(3) NIST SP 800-53 r5 - CA-5a NIST SP 800-53 r5 - CA-5b NIST SP 800-53 r5 - PM-4a NIST SP 800-53 r5 - PM-4b Veterans Affairs Cybersecurity Program Directive 6500 - a(2)(g) Veterans Affairs Cybersecurity Program Directive 6500 - d(4)(b)

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization: develops and submits a Plan of Action and Milestones (POA&M) in accordance with federal reporting requirements by the OMB for the information system within 30 days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. The organization implements a process to ensure that plans of action and milestones (POA&M) for the security program and associated organizational information systems are reported in accordance with organizational and CMS reporting requirements.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization updates the Plan of Action and Milestones (POA&M) at least monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation (example):	The organization implements processes to measure risks to guide its recommendations for and use of mitigating controls using threat analysis tools (e.g., event trees, attack trees, kill chains) in understanding and supporting the measurement of information security risks.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization submits an updated Corrective Action Plan (CAP) to the appropriate federal and state agencies twice each year to address corrective actions identified during an on-site safeguards review until all findings are closed. The CAP is submitted as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date. The organization ensures the individual and/or office responsible for correcting each weakness is identified in the appropriate POA&M.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization employs automated mechanisms to help ensure that the Plan of Action and Milestones (POA&M) for the information system is accurate, up to date, and readily available.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The organization develops a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system, and updates the existing plan of action and milestones at least quarterly based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
Level ISO/IEC 23894 Implementation Requirements	
Level ISO/IEC 23894 Implementation (example):	As part of the risk management process, the organization identifies key controls relevant to its development and/or use of AI systems.

	The organization, using a risk-based process, identifies, assesses, understands, and takes appropriate treatment measures to address the AI risks to which they are exposed.
Level ISO 31000 Implementation Requirements	
Level ISO 31000 Implementation (example):	The organization integrates risk treatment plans into the management plans and processes of the organization.
Control Reference: 03.d Risk Evaluation	
Control Specification:	Risks shall be continually evaluated and assessed.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The risk management process is integrated with the change management process.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC3.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) ISO/IEC 27799:2016 12.1.2 NIST Cybersecurity Framework v1.1 - ID.RA-1

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	Risk assessments are re-evaluated at least annually, or when there are significant changes in the environment. Risk assessments are conducted whenever there is a significant change in the environment, or a change that could have a significant impact. Results of the risk assessments are included in the change management process, so they may guide the decisions within the change management process (e.g., approvals for changes).
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC3.4 AICPA Trust Services Criteria - AICPA 2017 CC4.1 AICPA Trust Services Criteria - AICPA 2017 CC8.1 Banking Requirements - FFIEC IS v2016 A.7.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-03 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(A) IRS Pub 1075 - PM-9c ISO/IEC 27001:2022 - 10.2e ISO/IEC 27001:2022 - 10.2g ISO/IEC 27001:2022 - 6.1.2a2 ISO/IEC 27001:2022 - 8.2a ISO/IEC 27799:2016 12.1.2 NIST Cybersecurity Framework v1.1 - ID.RA-5 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-171 r2 - 3.4.4[a] NY OHIP Moderate-Plus Security Baseline v5.0 - CA-6[IS.1e]

Level ISO/IEC 23894 Implementation Requirements	
Level ISO/IEC 23894 Implementation (example):	The organization identifies, quantifies or qualitatively describes, and prioritizes AI risk against risk criteria and objectives.

Control Category: 04.0 - Security Policy

Objective Name: 04.01 Information Security Policy

Control Objective:	To provide management direction in line with business objectives and relevant laws and regulations, demonstrate support for, and commitment to information security through the issue and maintenance of information security policies across the organization.

Control Reference: 04.a Information Security Policy Document

Control Specification:	Information Security Policy documents shall be approved by management, published, and communicated to all employees and relevant external parties. Information Security Policy documents shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy documents shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA The Joint Commission v2016 PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The organization’s information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management’s commitment; describe management and workforce members’ roles and responsibilities; and establish the organization’s approach to managing information security.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.3 AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC2.3 AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC5.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) COBIT 5 APO13.02 COBIT 5 DS5.2 Health Industry Cybersecurity Practices - 10.M.A Health Industry Cybersecurity Practices - 10.S.A HIPAA Privacy Rule - 164.530(i)(1) HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) HITRUST ISO/IEC 27001:2022 - 5.1d ISO/IEC 27001:2022 - 5.2a ISO/IEC 27001:2022 - 5.2c ISO/IEC 27001:2022 - 5.2d ISO/IEC 27001:2022 - 5.2e ISO/IEC 27001:2022 - 5.2f ISO/IEC 27001:2022 - 5.2g ISO/IEC 27001:2022 - 6.2a ISO/IEC 27002:2022 - 5(1) ISO/IEC 27002:2022 - 5(2) ISO/IEC 27002:2022 - 5(4) ISO/IEC 27799:2016 5.1.1 NIST Cybersecurity Framework v1.1 - ID.GV-1 NIST Cybersecurity Framework v1.1 - ID.GV-3 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-3(9)[NYS.1b] The Joint Commission (v2016) - TJC IM.02.01.03, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust

Level 2 Implementation (example):	As applicable to the focus of a security policy particular document, security policies contain: the organization's mission, vision, values, objectives, activities, and purpose, including the organization's place in critical infrastructure; a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; a framework for setting control objectives and controls, including the structure of risk assessment and risk management; the need for information security; the goals of information security; the organization's compliance scope; legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination; a definition of general and specific responsibilities for information security management, including reporting information security incidents; references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users comply with); a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including but not limited to CSF control objectives such as: (a) compliance with legislative, regulatory, and contractual requirements; (b) security education, training, and awareness requirements for the workforce, including researchers and research participants; (c) incident response and business continuity management; (d) consequences of information security policy violations; (e) continuous monitoring; (f) designating and maintaining an appropriately resourced and technically experienced information security team; (g) physical security of areas where sensitive information (e.g., PII, PCI and PMI data); and (h) coordination among organizational entities. As applicable to the focus of a security policy particular document, security policies also prescribe the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.3 AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC2.3 AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC5.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) COBIT 5 APO13.02 COBIT 5 DS5.2 HIPAA Privacy Rule - 164.530(i)(1) HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) HITRUST IRS Pub 1075 - PM-18a ISO/IEC 27001:2022 - 4.3d ISO/IEC 27001:2022 - 6.2a ISO/IEC 27001:2022 - 7.5.1a ISO/IEC 27001:2022 - 7.5.1b ISO/IEC 27799:2016 5.1.1 NIST Cybersecurity Framework v1.1 - ID.GV-1 NIST Cybersecurity Framework v1.1 - ID.GV-3 The Joint Commission (v2016) - TJC IM.02.01.03, EP 1 Veterans Affairs Cybersecurity Program Directive 6500 - a(3)(d) Veterans Affairs Cybersecurity Program Directive 6500 - a(3)(h) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(a)

Level FTI Custodians Implementation Requirements

Level PCI Implementation Requirements

Level PCI Implementation (example):	The organization ensures that policies are documented, communicated and in use for the following: managing firewalls; managing vendor defaults and other security parameters; protecting stored cardholder data; encrypting transmissions of cardholder data; protecting systems against malware; developing and maintaining secure systems and applications; restricting access to cardholder data; identification and authentication; restricting physical access to cardholder data; monitoring access to network resources and cardholder data; and security monitoring and testing.

Level DGF Implementation Requirements	
Level DGF Implementation (example):	Data Governance policies, rules, and standards are explicitly defined, documented, and communicated.

Control Reference: 04.b Review of the Information Security Policy

Control Specification:	The information security policy documents shall be reviewed at planned intervals or if significant changes occur to ensure its continuing adequacy and effectiveness.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA Texas Medical Records Privacy Act
Level 1 Implementation (example):	The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Security policies are communicated throughout the organization.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(a) 23 NYCRR 500 - 500.08(b) AICPA Trust Services Criteria - AICPA 2017 CC1.4 AICPA Trust Services Criteria - AICPA 2017 CC5.2 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) Health Industry Cybersecurity Practices - 10.M.A HIPAA Privacy Rule - 164.530(b)(2)(i)(C) HIPAA Privacy Rule - 164.530(i)(2)(i) HIPAA Privacy Rule - 164.530(i)(2)(iii) HIPAA Privacy Rule - 164.530(i)(4)(i)(A) HIPAA Privacy Rule - 164.530(i)(4)(i)(B) HIPAA Privacy Rule - 164.530(i)(5)(i) HIPAA Privacy Rule - 164.530(j)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(iii) ISO/IEC 27002:2022 - 5(1) ISO/IEC 27799:2016 5.1.2
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)

Level 2 Implementation (example):	A process is defined, and implemented for individuals to make complaints concerning the information security policies and procedures or the organization's compliance with the policies and procedures. All complaints and requests for changes are documented, along with their disposition, if any. The information security policy documents have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. Policies are reviewed no less than every 365 days or if significant changes occur in the operating or business environment, updated/improved based on specific feedback (e.g., prior reviews, incidents and preventative/corrective actions), and approved by an appropriate level of management. The input to the management review includes information on: feedback from interested parties; results of independent reviews; status of preventive and corrective actions; results of previous management reviews; process performance and information security policy compliance; changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment; trends related to threats and vulnerabilities; reported information security incidents; and recommendations provided by relevant authorities.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC5.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IP-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) HIPAA Privacy Rule - 164.530(d)(1) HIPAA Privacy Rule - 164.530(d)(2) HIPAA Privacy Rule - 164.530(i)(2)(iii) HIPAA Privacy Rule - 164.530(i)(3) HIPAA Privacy Rule - 164.530(i)(4)(i)(B) HIPAA Privacy Rule - 164.530(i)(5)(i) HIPAA Privacy Rule - 164.530(i)(5)(ii) HIPAA Security Rule - § 164.308(a)(1)(i) ISO/IEC 27001:2022 - 7.5.2c ISO/IEC 27799:2016 5.1.2 NIST Cybersecurity Framework v1.1 - ID.GV-1 PCI DSS v3.2.1 12.1.1

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	DirectTrust EHNAC Banking Requirements
Level 3 Implementation (example):	Management's risk profile review addresses: the changing nature of the organization's operations and thus risk profile and risk management needs; the changes made to the IT infrastructure of the organization, along with the changes these bring to the organization's risk profile; the changes identified in the external environment that similarly impact the organization's risk profile; the latest controls, compliance and assurance requirements from arrangements of national bodies and of new legislation or regulation; the latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; the results of legal cases tested in courts that thereby establish or cancel precedents and established practices; and the challenges and issues regarding the policy, as expressed to the organization by its staff, customers, and their partners and care givers, researchers, and governments, e.g., privacy commissioners.
Level 3 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.4.5 FTC Red Flags Rule (16 CFR 681) - 681.A2.c1 FTC Red Flags Rule (16 CFR 681) - 681.A6.b1 FTC Red Flags Rule (16 CFR 681) - 681.A6.b2 HIPAA Privacy Rule - 164.530(i)(4)(i)(A) HIPAA Privacy Rule - 164.530(i)(4)(ii)(A) HIPAA Security Rule - § 164.316(b)(2)(iii) ISO/IEC 27001:2022 - 4.1 ISO/IEC 27001:2022 - 4.2a ISO/IEC 27001:2022 - 4.2b ISO/IEC 27001:2022 - 4.3a ISO/IEC 27001:2022 - 4.3b ISO/IEC 27001:2022 - 6.1.1a ISO/IEC 27001:2022 - 9.3.2b ISO/IEC 27001:2022 - 9.3.2c ISO/IEC 27001:2022 - 9.3.2e ISO/IEC 27799:2016 5.1.2 Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(a) Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(f)

Level FTI Custodians Implementation Requirements	

Level DGF Implementation Requirements	
Level DGF Implementation (example):	Data Governance policies, rules, and standards are updated as needed or at least annually.

Control Category: 05.0 - Organization of Information Security

Objective Name: 05.01 Internal Organization

Control Objective:	To maintain the security of the organization's information and information assets (data centers or offices that process covered information).
Control Reference: 05.a Management Commitment to Information Security	
Control Specification:	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA The Joint Commission v2016 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	A senior-level information security official is appointed. The senior-level information security official is responsible for ensuring the organization's information security processes are in place, communicated to all stakeholders, and consider and address organizational requirements.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.04(a)(1) Banking Requirements - FFIEC IS v2016 A.1.5 Banking Requirements - FFIEC IS v2016 A.2.3 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-02 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 DS5.1 FedRAMP - CA-6a[H] FedRAMP - CA-6a[L] FedRAMP - CA-6a[M] HIPAA Security Rule - § 164.308(a)(2) HITRUST De-ID Framework - De-ID Framework v1 Accountable Individuals: General HITRUST De-ID Framework - De-ID Framework v1 Security Points of Contact: General IRS Pub 1075 - PM-2 ISO/IEC 27001:2022 - 4.2b ISO/IEC 27001:2022 - 4.2c ISO/IEC 27001:2022 - 7.4d MARS-E v2.2 - PM-2 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-29[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-29a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-29b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9[IS.1b] PCI DSS v3.2.1 12.5 PCI DSS v3.2.1 12.5.1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(a) The Joint Commission (v2016) - TJC IM.02.01.03, EP 5
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) The Joint Commission v2016 23 NYCRR 500 Banking Requirements PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	Senior management: formally appoints a senior-level information security official for the development, implementation, and administration of security matters; formally establishes and communicates the organization's priorities for organizational mission, objectives, and activities; ensures that the organization's information security processes are in place; ensures that the organization's information security processes are communicated to all stakeholders; formally ensures that the organization's information security processes consider and address organizational requirements; formally assigns an organization single point of contact or group to provide program oversight (governance), review and update the organizations security plan (strategy, policies, etc.), ensure compliance with the security plan by the workforce, and evaluate and accept information security risk on behalf of the organization (e.g., CEO, COO, Security Steering Committee, etc.); formulates, reviews, and approves information security policies and a policy exception process; periodically, at a minimum, annually, reviews and assesses the effectiveness of the implementation of the information security policy; provides clear direction and visible management support for security initiatives; provides the resources needed for information security; initiates plans and programs to maintain information security awareness; ensures that all appropriate measures are taken to avoid cases of identity theft targeted at clients/customers, employees, and third parties; ensures that the implementation of information security controls is coordinated across the organization; and determines and coordinates, as needed, internal or external information security specialists, and review and coordinate results of the specialists' advice throughout the organization. Senior management formally appoints security specialists and reviews and coordinates results of the security specialists' advice throughout the organization.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(a) 23 NYCRR 500 - 500.03(b) 23 NYCRR 500 - 500.03(c) 23 NYCRR 500 - 500.03(d) 23 NYCRR 500 - 500.03(e) 23 NYCRR 500 - 500.03(f) 23 NYCRR 500 - 500.03(g) 23 NYCRR 500 - 500.03(h) 23 NYCRR 500 - 500.03(i) 23 NYCRR 500 - 500.03(j) 23 NYCRR 500 - 500.03(k) 23 NYCRR 500 - 500.03(l) 23 NYCRR 500 - 500.03(m) 23 NYCRR 500 - 500.03(n) 23 NYCRR 500 - 500.04(a)(1) 23 NYCRR 500 - 500.04(a)(2) 23 NYCRR 500 - 500.04(a)(3) 23 NYCRR 500 - 500.04(b)(1) 23 NYCRR 500 - 500.04(b)(2) 23 NYCRR 500 - 500.04(b)(3) 23 NYCRR 500 - 500.04(b)(4) 23 NYCRR 500 - 500.04(b)(5) 23 NYCRR 500 - 500.10(a)(1) 23 NYCRR 500 - 500.10(a)(2) 23 NYCRR 500 - 500.10(a)(3) 23 NYCRR 500 - 500.10(b) AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC3.2 Banking Requirements - FFIEC IS v2016 A.1.5 Banking Requirements - FFIEC IS v2016 A.2.10 Banking Requirements - FFIEC IS v2016 A.2.2 Banking Requirements - FFIEC IS v2016 A.2.3 Banking Requirements - FFIEC IS v2016 A.2.6 Banking Requirements - FFIEC IS v2016 A.2.9 Banking Requirements - FFIEC IS v2016 A.6.2 Banking Requirements - FFIEC IS v2016 A.6.4(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-13 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 HIPAA Security Rule - § 164.308(a)(2) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) HIPAA Security Rule - § 164.316(b)(2)(iii) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Accountable Individuals: General HITRUST De-ID Framework - De-ID Framework v1 Security Points of Contact: General IRS Pub 1075 - PM-3a IRS Pub 1075 - PM-3b IRS Pub 1075 - PM-3c ISO/IEC 27001:2022 - 4.1

Level 2 Authoritative Source Mapping (Cont.):	ISO/IEC 27001:2022 - 4.2c ISO/IEC 27001:2022 - 4.3c ISO/IEC 27001:2022 - 5.1a ISO/IEC 27001:2022 - 5.1h ISO/IEC 27001:2022 - 5.3b ISO/IEC 27001:2022 - 6.1.1e1 ISO/IEC 27001:2022 - 7.2a ISO/IEC 27001:2022 - 7.2d ISO/IEC 27001:2022 - 9.3.2d4 ISO/IEC 27799:2016 5.1.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PM-3a MARS-E v2.2 - PM-3b MARS-E v2.2 - PM-3c MARS-E v2.2 - PM-9b MARS-E v2.2 - SA-2d NIST Cybersecurity Framework v1.1 - ID.BE-2 NIST Cybersecurity Framework v1.1 - ID.BE-3 NIST Cybersecurity Framework v1.1 - ID.RM-1 NIST Cybersecurity Framework v1.1 - ID.RM-2 NIST Cybersecurity Framework v1.1 - PR.IP-8 NIST SP 800-53 R4 AC-3(4)[S]{2} NIST SP 800-53 R4 CM-3g[HM]{3} NIST SP 800-53 R4 PL-9[S]{0} NIST SP 800-53 R4 PM-3[HML]{0} NIST SP 800-53 r5 - AC-3(4) NIST SP 800-53 r5 - CA-2c NIST SP 800-53 r5 - CM-3g NIST SP 800-53 r5 - PM-3a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-2 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-2[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-3[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-3[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-3[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-3a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-3b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-3c NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9[IS.1d] PCI DSS v3.2.1 12.5 PCI DSS v3.2.1 12.5.1 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5 Veterans Affairs Cybersecurity Program Directive 6500 - a(3)(f)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	

Level 3 Regulatory Factors:	FedRAMP HITRUST De-ID Framework
Level 3 Implementation (example):	The organization: formally creates a dedicated security management forum; publishes the dedicated security management forum's member list; and publishes the dedicated security management forum's charter. The organization conducts an annual assessment of the effectiveness of its security program performed by a qualified outside organization.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.4 AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC5.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) Health Industry Cybersecurity Practices - 10.S.A HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(8) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Governance: General ISO/IEC 27799:2016 18.2.1 ISO/IEC 27799:2016 5.1.1 NIST Cybersecurity Framework v1.1 - DE.DP-3 NIST Cybersecurity Framework v1.1 - DE.DP-4
Level PCI Implementation Requirements	
Level PCI Implementation (example):	When being assessed as a service provider, the organization's executive management establishes: responsibility for the protection of cardholder data; a PCI DSS compliance program which includes overall accountability for maintaining PCI DSS compliance; a PCI DSS compliance program which includes defining a charter for a PCI DSS compliance program; and a PCI DSS compliance program which includes communication to executive management.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	The compliance and success of the Data Governance program is evaluated at the organization. The application levels and reports on such attributes are shared with the leadership periodically.

	The individuals performing Data Governance work have the skills, experience, and necessary training to implement Data Governance processes/activities, as evidenced by knowledge of the tools, processes, corporate policies, and business expectations around management of the data.

Control Reference: 05.b Information Security Coordination

Control Specification:	Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	The Joint Commission v2016
Level 1 Implementation (example):	Security activities (e.g., implementing controls, correcting nonconformities) are coordinated in advance and communicated across the entire organization where necessary.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) Banking Requirements - FFIEC IS v2016 A.1.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-02(03) (HIGH; MOD) COBIT 5 APO13.02 COBIT 5 DS5.1 HIPAA Security Rule - § 164.308(a)(6)(i) The Joint Commission (v2016) - TJC IM.02.01.03, EP 8

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA The Joint Commission v2016 Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The organization determines information security requirements for the information system in mission/business process planning, documents and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process, establishes a discrete line item for information security in organizational programming and budgeting information, and assigns authority and accountability to resources for communicating threat information. Information security coordination: involves active cooperation and collaboration across the entire organization; ensures that security activities across the entire organization are executed in compliance with the information security policy; ensures that security policy deviations are identified and reviewed; identifies how to handle non-compliance (such as sanctions or disciplinary action); assesses the adequacy of the implementation of information security controls; coordinates the implementation of information security controls; effectively promotes information security education, training, and awareness throughout the organization; ensures that threat information has been communicated to identified internal stakeholders; and ensures that threat information has been communicated to identified external stakeholders.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.1 AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC3.4 Banking Requirements - FFIEC IS v2016 A.1.5 Banking Requirements - FFIEC IS v2016 A.3.1 Banking Requirements - FFIEC IS v2016 A.3.1c Banking Requirements - FFIEC IS v2016 A.8.1(n) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-02(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-02 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 FedRAMP - PL-2a1[H] FedRAMP - PL-2a1[L] FedRAMP - PL-2a1[M] FedRAMP - PL-2a2[H] FedRAMP - PL-2a2[L] FedRAMP - PL-2a2[M] FedRAMP - PL-2a3[H] FedRAMP - PL-2a3[L] FedRAMP - PL-2a3[M] FedRAMP - PL-2a4[H] FedRAMP - PL-2a4[L] FedRAMP - PL-2a4[M] FedRAMP - PL-2a5[H] FedRAMP - PL-2a5[L] FedRAMP - PL-2a5[M] FedRAMP - PL-2a6[H] FedRAMP - PL-2a6[L] FedRAMP - PL-2a6[M] FedRAMP - PL-2a7[H] FedRAMP - PL-2a7[L] FedRAMP - PL-2a7[M] FedRAMP - PL-2a8[H] FedRAMP - PL-2a8[L] FedRAMP - PL-2a8[M] FedRAMP - PL-2a9[H] FedRAMP - PL-2a9[L] FedRAMP - PL-2a9[M] FedRAMP - PL-2b[H] FedRAMP - PL-2b[L] FedRAMP - PL-2b[M] FedRAMP - PL-2e[H] FedRAMP - PL-2e[L] FedRAMP - PL-2e[M] FedRAMP - SA-2a[H] FedRAMP - SA-2a[L] FedRAMP - SA-2a[M] FedRAMP - SA-2b[H] FedRAMP - SA-2b[L] FedRAMP - SA-2b[M] FedRAMP - SA-2c[H] FedRAMP - SA-2c[L] FedRAMP - SA-2c[M]

Level 2 Authoritative Source Mapping (Cont.):	HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.316(b)(2)(iii) IRS Pub 1075 - PM-18b ISO/IEC 27001:2022 - 4.2a ISO/IEC 27001:2022 - 4.3a ISO/IEC 27001:2022 - 4.3b ISO/IEC 27001:2022 - 4.3c ISO/IEC 27001:2022 - 5.1f ISO/IEC 27001:2022 - 7.4a ISO/IEC 27001:2022 - 7.4b ISO/IEC 27001:2022 - 7.4c ISO/IEC 27001:2022 - 7.4d ISO/IEC 27001:2022 - 8.1a ISO/IEC 27002:2022 - 5(35) ISO/IEC 27002:2022 - 8(26) MARS-E v2.2 - PL-2b MARS-E v2.2 - PL-2e MARS-E v2.2 - PM-16 MARS-E v2.2 - SA-2a MARS-E v2.2 - SA-2b MARS-E v2.2 - SA-2c NIST Cybersecurity Framework v1.1 - ID.BE-3 NIST Cybersecurity Framework v1.1 - ID.GV-4 NIST Cybersecurity Framework v1.1 - RC.CO-3 NIST SP 800-171 r2 - 3.12.4[a] NIST SP 800-171 r2 - 3.12.4[b] NIST SP 800-171 r2 - 3.12.4[c] NIST SP 800-171 r2 - 3.12.4[d] NIST SP 800-171 r2 - 3.12.4[e] NIST SP 800-171 r2 - 3.12.4[g] NIST SP 800-171 r2 - 3.12.4[h] NIST SP 800-53 R4 AC-17(6)[S]{1} NIST SP 800-53 R4 CA-2c[HML]{0} NIST SP 800-53 R4 CA-2d[HML]{0} NIST SP 800-53 R4 PL-2b[HML]{0} NIST SP 800-53 R4 PL-2e[HML]{0} NIST SP 800-53 R4 PM-11a[HML]{0} NIST SP 800-53 R4 PM-6[HML]{0} NIST SP 800-53 R4 SA-2[HML]{0} NIST SP 800-53 R4 SI-5(1)[H]{0} NIST SP 800-53 R4 SI-6(2)[S]{0} NIST SP 800-53 R4 SI-6(3)[S]{0} NIST SP 800-53 r5 - AC-17(6) NIST SP 800-53 r5 - CA-2e NIST SP 800-53 r5 - CA-2f NIST SP 800-53 r5 - PL-2b NIST SP 800-53 r5 - PL-2e NIST SP 800-53 r5 - PL-8a1 NIST SP 800-53 r5 - PM-6 NIST SP 800-53 r5 - SA-2 NIST SP 800-53 r5 - SI-5(1) NIST SP 800-53 r5 - SI-6(2) NIST SP 800-53 r5 - SI-6(3) NIST SP 800-53 r5 - SR-2c NY OHIP Moderate-Plus Security Baseline v5.0 - AC-3(9)[NYS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-3(9)[NYS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-17b NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4[IS.2]

Level 2 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4[PHI.2] PCI DSS v3.2.1 12.5.2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 8 Veterans Affairs Cybersecurity Program Directive 6500 - a(5)(f) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(e) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(l)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation (example):	The organization convenes an internal meeting for the organization's security single point of contact and the organizational area/business unit security contacts on a monthly or near-to-monthly basis.
Level 3 Authoritative Source Mapping:	NIST Cybersecurity Framework v1.1 - PR.IP-8
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization establishes a discrete line item in CMS programming and budgeting documentation for the implementation and management of information systems security. The organization develops a security plan for the information system that is consistent with the CMS System Security Plan (SSP) Procedure.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	Security plans are reviewed at least annually, when changes are made to the information system or information protection requirements, or when incidents occur that impact the plans' validity.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization: advises the IRS of future actions that will affect the organizations current efforts to ensure the confidentiality of FTI; certifies to the IRS that the organization is protecting FTI pursuant to IRC Section 6103(p)(4); and certifies to the IRS that the organization is protecting FTI pursuant to the organizations own security requirements.

	Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor (e.g., cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, information technology support, or tax modeling or revenue forecasting providers), or at least forty-five (45) days prior to the disclosure of FTI, to ensure that appropriate contractual language is included and that contractors are held to safeguarding requirements. Any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any disclosures to subcontractors.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The security plan for the information system: is consistent with the RMH Procedures; is consistent with the organization's enterprise architecture; explicitly defines the authorization boundary for the system; describes the operational context of the information system in terms of missions and business processes; provides the security categorization of the information system including supporting rationale; describes the operational environment for the information system and relationships with or connections to other information systems; provides an overview of the security requirements for the system; identifies any relevant overlays, if applicable; describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and is reviewed and approved by the authorizing official or designated representative prior to plan implementation. The organization updates the security plan: minimally every three years, to address current conditions; whenever there are significant changes to the information system/environment of operation that affect security; whenever problems are identified during plan implementation or security control assessments; whenever the data sensitivity level increases; after a serious security violation due to changes in the threat environment; and before the previous security authorization expires.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	The stakeholders impacted by Data Governance are well understood. Funding for Data Governance activities are budgeted and provided for.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization defines organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation, determines information protection and PII processing needs arising from the defined mission and business processes, and reviews and revises the mission and business processes annually.
Level ISO/IEC 23894 Implementation Requirements	

Control Reference: 05.c Allocation of Information Security Responsibilities

Control Specification:	All information security responsibilities shall be clearly defined.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	HITRUST De-ID Framework PCI DSS v3.2.1 Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization clearly allocates and assigns responsibilities to identify and protect individual IT assets in accordance with the security policies. Where necessary, the organization supplements policies with more detailed guidance for specific assets and facilities. When security responsibilities are delegated to others, the individual originally assigned these responsibilities remains accountable, and the organization determines that any delegated tasks have been correctly performed.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC5.3 Banking Requirements - FFIEC IS v2016 A.1.5 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.8 Banking Requirements - FFIEC IS v2016 A.2.9 COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 Health Industry Cybersecurity Practices - 10.M.A PCI DSS v3.2.1 12.4
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) HITRUST De-ID Framework Banking Requirements PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate

Level 2 Implementation (example):	The organizations senior-level information security official coordinates, develops, implements, and maintains an organization-wide information security program. The organization formally assigns the following specific information security responsibilities to an individual or team: establishment, documentation and distribution of security policies and procedures; monitoring and analyzing security alerts and information, and distributing security alerts, information and analysis to appropriate personnel; establishment, documentation and distribution of security incident response and escalation procedures to ensure timely and effective handling of all situations; administering user accounts, including additions, deletions and modifications; and monitoring and controlling all access to data. Information security roles and responsibilities are coordinated and aligned with internal roles, and external partners. The organization identifies, by name or position, non-professional or professional security contacts in each major organizational area or business unit. The organization clearly defines the roles of each security contact including the administration and implementation of the organization's security programs, responsibilities of each security contact including the administration and implementation of the organization's security programs, and authority of each security contact including the administration and implementation of the organization's security programs. Each security contact annually documents compliance related to identified legal requirements, reports to the organization's single point of contact for security, provides evaluations on the effectiveness of the policies and procedures implemented in addressing risk, provides evaluations of service provider arrangements, provides significant incidents and the response, and provides recommendations for material changes to the security programs for which they are responsible. The organization's single point of contact for security matters provides supplemental security awareness and training. Security contacts are responsible for reviewing reports related to the security organization, network, systems and programs implemented, and formally approving any material changes to these items prior to implementation.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.3 Banking Requirements - FFIEC IS v2016 A.1.5 Banking Requirements - FFIEC IS v2016 A.2.7 Banking Requirements - FFIEC IS v2016 A.2.8 Banking Requirements - FFIEC IS v2016 A.2.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-10 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 FedRAMP - SA-3c[H] FedRAMP - SA-3c[L] FedRAMP - SA-3c[M] FTC Red Flags Rule (16 CFR 681) - 681.A6.a1 FTC Red Flags Rule (16 CFR 681) - 681.A6.a2 FTC Red Flags Rule (16 CFR 681) - 681.A6.a3 FTC Red Flags Rule (16 CFR 681) - 681.A6.b1 FTC Red Flags Rule (16 CFR 681) - 681.A6.b2 HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(2) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.316(b)(1)(i) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Accountable Individuals: General IRS Pub 1075 - PM-19 IRS Pub 1075 - PM-29a IRS Pub 1075 - PM-29b ISO/IEC 27001:2022 - 7.2a ISO/IEC 27001:2022 - 7.2b ISO/IEC 27001:2022 - 7.2c ISO/IEC 27001:2022 - 7.2d ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 6.1.3 MARS-E v2.2 - IR-7(2)b MARS-E v2.2 - PM-4a1 NIST Cybersecurity Framework v1.1 - ID.GV-2 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST SP 800-53 R4 PM-2[HML]{0} NIST SP 800-53 R4 SA-3c[HML]{0} NIST SP 800-53 r5 - PM-2 NIST SP 800-53 r5 - SA-3c PCI DSS v3.2.1 12.4 PCI DSS v3.2.1 12.5 PCI DSS v3.2.1 12.5.1 PCI DSS v3.2.1 12.5.2 PCI DSS v3.2.1 12.5.3 PCI DSS v3.2.1 12.5.4 PCI DSS v3.2.1 12.5.5

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP
Level 3 Implementation (example):	The organization specifically defines the roles and responsibilities of each security contact in writing.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-03 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(2) ISO/IEC 27799:2016 6.1.1 NIST Cybersecurity Framework v1.1 - DE.DP-1 NIST Cybersecurity Framework v1.1 - RS.CO-1
Level DGF Implementation Requirements	
Level DGF Implementation (example):	The organization has identified an executive owner responsible for the Data Governance program, goals, and implementation roadmap.

Control Reference: 05.d Authorization Process for Information Assets and Facilities

Control Specification:	A management authorization process for new information assets (e.g., systems and applications) (see Other Information), and facilities (e.g., data centers or offices where covered information is to be processed) shall be defined and implemented.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	

Level 1 Regulatory Factors:	FISMA High Low Moderate
Level 1 Implementation (example):	Management formally authorizes (approves) new information assets and facilities for processing (use) before commencing operations and periodically reviews and updates authorizations (approvals) at a frequency defined by the organization – but no less than three years.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-06 (HIGH; MOD) FedRAMP - CA-6b[H] FedRAMP - CA-6b[L] FedRAMP - CA-6b[M] FedRAMP - CA-6c[H] FedRAMP - CA-6c[L] FedRAMP - CA-6c[M] HIPAA Security Rule - § 164.308(a)(4)(ii)(C) NIST SP 800-53 R4 CA-6[HML]{0} NIST SP 800-53 r5 - CA-6a NIST SP 800-53 r5 - CA-6c2 NIST SP 800-53 r5 - CA-6e

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	Supplemental
Level 2 Implementation (example):	The following is required for the authorization process for information assets and facilities: new information processing assets (internal to the organization or via a service provided by a third-party) have appropriate user management authorization of their purpose and use; authorization is also obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met; information assets have appropriate security measures commensurate with the type of information it will store, process, or transmit; the assets address compliance with all applicable laws, regulations, standards, policies, and other applicable sections of the HITRUST CSF; hardware and software is checked to ensure that they are compatible with other system components; and the use of personal or privately owned information processing equipment (e.g., laptops, home-computers, or hand-held devices) for processing business information, may introduce new vulnerabilities and necessary controls are identified and implemented.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-10 (HIGH; MOD) NIST SP 800-53 R4 PE-20b[S]{1} NIST SP 800-53 R4 SA-13a[S]{1}

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP
Level 3 Implementation (example):	All facilities undergo a site security survey, prior to lease or purchase, by the organization's security department or a trusted third-party. The organization resolves all security shortcomings before any covered information is processed at that location. All sites that process covered information are reviewed whenever the site undergoes a significant change in mission or makes substantive physical changes in its facilities or workforce and no less than annually.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC3.4 AICPA Trust Services Criteria - AICPA 2017 CC8.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-03 (HIGH; MOD) NIST Cybersecurity Framework v1.1 - ID.RA-4

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization: ensures that the authorizing official authorizes the information system for processing before commencing operations; updates the security authorization within every three years; updates the security authorization when significant changes are made to the system; updates the security authorization when changes in requirements result in the need to process data of a higher sensitivity; updates the security authorization when changes occur to authorizing legislation or federal requirements; updates the security authorization after the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; updates the security authorization prior to expiration of a previous security authorization.

Level FTI Custodians Implementation Requirements	

Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization ensures that the authorizing official authorizes the information system for processing before commencing operations. A senior organization official signs the systems Authority to Operate (ATO) before commencing operations. If the organization maintains a system-to-system connection with CMS through an executed interconnection security agreement (ISA), the CMS-granted Authority to Connect (ATC) is updated within every three years, when significant changes are made to the system, when changes in requirements result in the need to process data of a higher sensitivity, when changes occur to authorizing legislation or federal requirements, after the occurrence of a serious security violation, which raises questions about the validity of an earlier security authorization, and prior to the expiration of a previous security authorization.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization has assigned authority to the CMS CIO, CISO, and Senior Official for Privacy (SOP) to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CMS officer and CMS Security Operations, presents an unacceptable level of risk to the CMS enterprise and/or mission. The organization updates the security authorization when changes occur to authorizing legislation or federal requirements that impact the system.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization employs a joint authorization process for the system that includes multiple authorizing officials. The organization employs a joint authorization process for the system that includes multiple authorizing officials. At least one of the authorizing officials is from an organization external to the organization conducting the authorization.

Control Reference: 05.e Confidentiality Agreements

Control Specification:	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Requirements for confidentiality and non-disclosure agreements are reviewed at least annually and when changes occur that influence these requirements. Confidentiality and non-disclosure agreements comply with all applicable laws and regulations for the jurisdiction to which it applies.
Level 1 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.8(e) ISO/IEC 27002:2022 - 6(6) ISO/IEC 27799:2016 13.2.4

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	
Level 2 Implementation (example):	The organization publishes a list of representatives who are authorized to sign a non-disclosure agreement on behalf of the organization, and keeps the list up to date to reflect personnel changes and departures.
Level 2 Authoritative Source Mapping:	HITRUST
Level HIE Implementation Requirements	
Level HIE Implementation (example):	As part of the agreement with connecting organizations, the HIE specifies which organization owns the data, and any restrictions as part of that ownership such as retention, integrity, and accuracy of data as part of its agreement with connecting organizations. Further, if the HIE is the owner of the data, all federal and state requirements associated with the patients' information are met.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	Confidentiality or non-disclosure agreements: address the requirement to protect confidential information using legally enforceable terms; include a definition of the information to be protected (e.g., confidential information); include expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely; include required actions when an agreement is terminated; include responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know'); include disclosures required to be limited to the limited data set or the minimum necessary to accomplish the intended purpose of such use, disclosure, or request; include ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; include the permitted use of confidential information, and rights of the signatory to use information; include individuals' rights to obtain a copy of the individual's information in an electronic format; include individuals' rights to have the individual's information transmitted to another entity or person designated by the individual, provided the request is clear, conspicuous, and specific; include the right to audit and monitor activities that involve confidential information; include the process for notification and reporting of unauthorized disclosure or confidential information breaches; include terms for information to be returned or destroyed at agreement cessation; and include expected actions to be taken (i.e. penalties that are possible) in case of a breach of this agreement. The confidentiality agreements are applicable to all personnel accessing covered information.

Control Reference: 05.f Contact with Authorities

Control Specification:	Appropriate contacts with relevant authorities shall be maintained.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization includes key contacts including phone numbers and email addresses as part of its incident management and/or business continuity plan. The organization designates a point of contact to review the list at least annually to keep it current.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.8.1(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(7)(i) ISO/IEC 27799:2016 6.1.3 MARS-E v2.2 - CP-2a1
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP Banking Requirements
Level 2 Implementation (example):	The organization defines a plan with associated contact information for reporting security incidents to law enforcement if it is expected that laws may have been broken. Each group within the organization (e.g., information security) has procedures documented and implemented that specify when and by whom authorities (e.g., law enforcement, fire department, supervisory authorities) are contacted, and how identified information security incidents are reported in a timely manner if it is suspected that laws may have been broken.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC7.3 Banking Requirements - FFIEC IS v2016 A.8.1(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-04 (HIGH; MOD) HIPAA Privacy Rule - 164.512(j)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) ISO/IEC 27002:2022 - 5(5) ISO/IEC 27799:2016 6.1.3 NIST Cybersecurity Framework v1.1 - RS.CO-2 NIST Cybersecurity Framework v1.1 - RS.CO-3 Veterans Affairs Cybersecurity Program Directive 6500 - d(2)(a)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP Banking Requirements
Level 3 Implementation (example):	The organization includes key contacts including phone numbers and email addresses as part of its incident management and/or business continuity plan. The organization designates a point of contact to review the list of key contacts in its incident management and/or business continuity plan at least quarterly to keep it current.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.8.1(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) ISO/IEC 27799:2016 6.1.3 ISO/IEC 27799:2016 6.1.6
Control Reference: 05.g Contact with Special Interest Groups	
Control Specification:	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	

Level 1 System Factors:	
Level 1 Regulatory Factors:	High Low Moderate Supplemental
Level 1 Implementation (example):	Membership in organization-defined special interest groups or forums/services are considered as a means to: improve knowledge of best practices and stay up to date with relevant security information; ensure the understanding of the information security environment is current and complete (e.g., threat monitoring/intelligence services); receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; gain access to specialist information security advice; share and exchange information about new technologies, products, threats, or vulnerabilities; and provide suitable liaison points when dealing with information security incidents.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.4.3 Banking Requirements - FFIEC IS v2016 A.4.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-15 (HIGH; MOD) FedRAMP - IR-4(8)[H] Health Industry Cybersecurity Practices - 8.M.C Health Industry Cybersecurity Practices - 8.S.B IRS Pub 1075 - IR-4(8) ISO/IEC 27002:2022 - 5(6) ISO/IEC 27799:2016 6.1.4 MARS-E v2.2 - PM-15a MARS-E v2.2 - PM-15b MARS-E v2.2 - PM-15c MARS-E v2.2 - SI-4a1 NIST Cybersecurity Framework v1.1 - ID.RA-2 NIST Cybersecurity Framework v1.1 - PR.IP-8 NIST SP 800-53 R4 IR-4(8)[S]{2} NIST SP 800-53 R4 PM-15[HML]{0} NIST SP 800-53 R4 PM-16[HML]{0} NIST SP 800-53 r5 - IR-4(8) NIST SP 800-53 r5 - PM-15a NIST SP 800-53 r5 - PM-16 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15c NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16[IS.1c] Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(e) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(l) Veterans Affairs Cybersecurity Program Directive 6500 - d(2)(g)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FISMA Banking Requirements Supplemental Requirements CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Membership in special interest groups or forums/services is required and actively maintained. The organization has a process to quickly identify newly discovered security threats and vulnerabilities such as a credible subscription service and map new threats and vulnerabilities into its security policies, guidelines, and daily operational procedures.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.4.3 Banking Requirements - FFIEC IS v2016 A.4.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-15 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-05(01) (HIGH) FedRAMP - SI-5(1)[H] HIPAA Security Rule - § 164.308(a)(5)(ii)(A) ISO/IEC 27002:2022 - 5(7) ISO/IEC 27799:2016 6.1.4 NIST Cybersecurity Framework v1.1 - ID.RA-2 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST Cybersecurity Framework v1.1 - ID.RM-3 NIST Cybersecurity Framework v1.1 - PR.IP-8 NIST Cybersecurity Framework v1.1 - RS.AN-5 NIST SP 800-53 R4 IR-4(8)[S]{1} NIST SP 800-53 r5 - IR-4(8) NIST SP 800-53 r5 - PM-16(1) NIST SP 800-53 r5 - RA-3(2) NIST SP 800-53 r5 - RA-3(3) NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16(1) NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16[IS.1c] Supplemental Requirements - SR v6.4 1-0 Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(e) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(c)

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization implements security directives in accordance with established time frames or notifies CMS of the degree of noncompliance.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization: receives information system security alerts, advisories, and directives on an ongoing basis (for example, from the U.S. Computer Emergency Readiness Team); generates and disseminates security alerts, advisories, and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities; and implements security directives in accordance with established time frames, or notifies the business owner of the degree of noncompliance.

Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization: disseminates security alerts, advisories and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities; and implements security directives in accordance with established time frames or notifies the business owner of the degree of noncompliance.

Control Reference: 05.h Independent Review of Information Security

Control Specification:	The organization's approach to managing information security and its implementation (control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, at a minimum annually, or when significant changes to the security implementation occur.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FedRAMP HITRUST De-ID Framework Banking Requirements State of Massachusetts Data Protection Act (201 CMR 17.00)
Level 1 Implementation (example):	An independent review of the information security management program and information security controls is conducted at least annually or whenever there is a material change to the business practices that may implicate the security or integrity of records containing personal information.

Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC3.4 Banking Requirements - FFIEC IS v2016 A.10.1 Banking Requirements - FFIEC IS v2016 A.10.3(d) Banking Requirements - FFIEC IS v2016 A.10.6 Banking Requirements - FFIEC IS v2016 A.8.1(c) Banking Requirements - FFIEC IS v2016 A.9.1 Banking Requirements - FFIEC IS v2016 A.9.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02(01) (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(8) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.316(b)(1)(i) HITRUST De-ID Framework - De-ID Framework v1 Privacy Reviews/Audits: General ISO/IEC 27799:2016 18.2.1 NIST Cybersecurity Framework v1.1 - DE.DP-3 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(a) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(b)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	An independent review of the organization’s information security management program is initiated by management to ensure the continuing suitability, adequacy, and effectiveness of the organization’s approach to managing information security and privacy. The tests and methods used are sufficient to validate the effectiveness of the security plan. Independent security program reviews: include an assessment of the organizations adherence to its security plan; address the need for changes to the approach to security in light of evolving circumstances, including the policy and control objectives and other opportunities for improvement, including those based on regular vulnerability assessments (e.g., network scans and penetration testing); carefully control information security tests to limit the risks to confidentiality, integrity, and system availability; are carried out by individuals independent of the area under review (e.g., the internal audit function, an independent manager or a third-party organization specializing in such reviews); are carried out by individuals who have the appropriate skills and experience; and include notification requirements to confirm whom to inform within the organization about the timing and nature of the assessment. Independent security program reviews are recorded and reported to the management who initiated the review, and maintained for a predetermined period of time as determined by the organization, but not less than three years.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC4.2 AICPA Trust Services Criteria - AICPA 2017 P8.1 Banking Requirements - FFIEC IS v2016 A.10.1 Banking Requirements - FFIEC IS v2016 A.10.3(d) Banking Requirements - FFIEC IS v2016 A.10.5 Banking Requirements - FFIEC IS v2016 A.10.6 Banking Requirements - FFIEC IS v2016 A.2.1(a) Banking Requirements - FFIEC IS v2016 A.2.1(b) Banking Requirements - FFIEC IS v2016 A.2.1(c) Banking Requirements - FFIEC IS v2016 A.6.8(c) Banking Requirements - FFIEC IS v2016 A.8.1(c) Banking Requirements - FFIEC IS v2016 A.9.1 Banking Requirements - FFIEC IS v2016 A.9.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-07(01) (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(iii) HITRUST De-ID Framework - De-ID Framework v1 Privacy Reviews/Audits: General ISO/IEC 27001:2022 - 10.2a1 ISO/IEC 27001:2022 - 10.2a2 ISO/IEC 27001:2022 - 10.2b1 ISO/IEC 27001:2022 - 10.2b2 ISO/IEC 27001:2022 - 10.2c ISO/IEC 27001:2022 - 9.2.2f ISO/IEC 27001:2022 - 9.3.1 ISO/IEC 27001:2022 - 9.3.2d3 ISO/IEC 27001:2022 - 9.3.3a ISO/IEC 27002:2022 - 5(36) ISO/IEC 27799:2016 18.2.1 MARS-E v2.2 - AC-5a NIST Cybersecurity Framework v1.1 - DE.DP-3 NIST Cybersecurity Framework v1.1 - DE.DP-4 NIST Cybersecurity Framework v1.1 - ID.GV-4 NIST Cybersecurity Framework v1.1 - PR.IP-7 NIST Cybersecurity Framework v1.1 - PR.IP-8 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(b)

Level NYDOH Implementation Requirements

Level NYDOH Implementation (example):	The organization develops an information security and privacy control assessment plan that describes the: scope of the assessment; security and privacy controls and control enhancements under assessment (including information security and privacy changes enacted by HHS and CMS CIO/CISO directives); assessment procedures to be used to determine control effectiveness; assessment environment; assessment team; and roles and responsibilities.

	The organization assesses the security and privacy controls in the information system and its environment of operation, as defined in implementation standards, within every 365 days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standards to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

Objective Name: 05.02 External Parties

Control Objective:	To ensure that the security of the organization's information and information assets, are not reduced by the introduction of external party products or services.

Control Reference: 05.i Identification of Risks Related to External Parties

Control Specification:	The risks to the organization's information and information assets from business processes involving external parties shall be identified, and appropriate controls implemented before granting access.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No
Level 1 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	Access granted to external parties is limited to the minimum necessary, limited in duration, and is revoked when no longer needed.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.23 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04 (HIGH; MOD)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records

Level 2 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No
Level 2 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) 23 NYCRR 500 Banking Requirements CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Access to the organization's information and systems by external parties is not permitted until due diligence is carried out to identify any requirements for specific controls where access to sensitive information (e.g., covered information, cardholder data) by external parties is required prior to establishing a formal relationship with the service provider, the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement, all security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party, and it is ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets. All remote access connections between the organization and all external parties are secured via encrypted channels (e.g., VPN). Any covered information shared with an external party is encrypted prior to transmission.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC2.3 AICPA Trust Services Criteria - AICPA 2017 CC9.2 AICPA Trust Services Criteria - AICPA 2017 P6.1 AICPA Trust Services Criteria - AICPA 2017 P6.4 Banking Requirements - FFIEC IS v2016 A.3.3 Banking Requirements - FFIEC IS v2016 A.6.18(c) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.31(a) Banking Requirements - FFIEC IS v2016 A.6.31(b) Banking Requirements - FFIEC IS v2016 A.6.31(c) Banking Requirements - FFIEC IS v2016 A.6.31(e) Banking Requirements - FFIEC IS v2016 A.6.31(f) Banking Requirements - FFIEC IS v2016 A.6.31(g) Banking Requirements - FFIEC IS v2016 A.6.7(a) Banking Requirements - FFIEC IS v2016 A.6.7(d) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08(01) (HIGH; MOD) EU GDPR Article 32(4) HIPAA Privacy Rule - 164.504(e)(2)(ii)(D) HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) ISO/IEC 27001:2022 - 4.1 ISO/IEC 27001:2022 - 4.3c ISO/IEC 27002:2022 - 5(19) ISO/IEC 27002:2022 - 5(22) ISO/IEC 27799:2016 15.1.1 ISO/IEC 27799:2016 15.1.2 ISO/IEC 27799:2016 15.1.3 NIST Cybersecurity Framework v1.1 - ID.BE-1 NIST Cybersecurity Framework v1.1 - ID.SC-2 NIST SP 800-53 R4 SA-14[S]{1} NIST SP 800-53 r5 - IA-12(6) PCI DSS v3.2.1 12.8.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	23 NYCRR 500 Banking Requirements

Level 3 Implementation (example):	Due diligence of the external party includes interviews, document review, checklists, review certifications (e.g., HITRUST) or other remote means and is integrated with the execution of a non-disclosure agreement (NDA).
Level 3 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.3.3 Banking Requirements - FFIEC IS v2016 A.6.31(b) Banking Requirements - FFIEC IS v2016 A.6.31(d) PCI DSS v3.2.1 12.8.3 PCI DSS v3.2.1 2.6
Level Cloud Service Providers Implementation Requirements	
Level Cloud Service Providers Implementation (example):	Cloud service providers design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization takes additional actions (e.g., requiring background checks) for selected service provider personnel, examining ownership records, employing only providers for which it has had positive experiences, and conducting periodic/unscheduled visits to service provider facilities to ensure that the interests of external service providers for systems processing or storing covered information are consistent with and reflect organizational interests.
Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation (example):	The organization identifies factors that increase the risk from supply chain attacks and responds with the following risk mitigations: purchases are made only through reputable vendors who demonstrate an ability to control their own supply chains; hardware is reviewed for anomalies; software is reviewed through both automated software testing and code reviews; and regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups. If the organization outsources cloud computing or storage to a third-party service provider, the organization addresses the key elements of outsourced cloud computing implementation and risk management in accordance with the FFIEC IS Outsourced Cloud Computing statement.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization performs due diligence on incident management service providers to ensure the provider has a credible history and is capable of providing the necessary services, and re-evaluates the capabilities on a regular basis (e.g., prior to contract renewal).
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	Privacy requirements must be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage PII. The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization assesses supply chain risks associated with systems, system components, and system services.

Control Reference: 05.j Addressing Security When Dealing with Customers	
Control Specification:	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The following security term is addressed prior to giving customers access to any of the organization's assets: description of the product or service to be provided; the right to monitor, and revoke, any activity related to the organization's assets; the respective liabilities of the organization and the customer. It is ensured that the customer is aware of their obligations. It is ensured that the customer accepts the responsibilities and liabilities prior to accessing, processing, communicating, or managing the organization's information and information assets.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework CMS Minimum Security Requirements (High) Privacy
Level 2 Implementation (example):	The organization ensures that the public has access to information about its privacy activities and is able to communicate with its senior privacy official (e.g., Chief Privacy Officer, Chief Data Protection Officer).

	The following security terms related to asset protection are addressed prior to giving customers access to any of the organization's assets: procedures to protect the organization’s assets, including information and software, and management of known vulnerabilities; procedures to determine whether any compromise of the assets (e.g., loss or modification of data) has occurred; integrity; restrictions on copying and disclosing information; permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; an authorization process for user access and privileges; a statement that all access that is not explicitly authorized is forbidden; and a process for revoking access rights or interrupting the connection between systems. The following security terms related to security incident management are addressed prior to giving customers access to any of the organization’s assets: reporting of information inaccuracies (e.g., of personal details), information security incidents, and security breaches; notification of information inaccuracies (e.g., of personal details), information security incidents, and security breaches; and investigation of information inaccuracies (e.g., of personal details), information security incidents, and security breaches. The following security terms are addressed prior to giving customers access to any of the organization’s assets: a description of each service to be made available; the target level of service and unacceptable levels of service; the different reasons, requirements, and benefits for customer access; responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation), especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries; and intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work. Access by customers to the organization’s information is not provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 TR-03 (HIGH; MOD) HIPAA Privacy Rule - 164.504(e)(4)(i)(A) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.312(d) HIPAA Security Rule - § 164.314(a)(2)(i)(B) HIPAA Security Rule - § 164.314(a)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Transparency: General ISO/IEC 27001:2022 - 7.5.3g ISO/IEC 27799:2016 14.1.2 MARS-E v2.2 - TR-3a MARS-E v2.2 - TR-3b NIST Cybersecurity Framework v1.1 - ID.BE-1 NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST Cybersecurity Framework v1.1 - RC.CO-1 NIST Cybersecurity Framework v1.1 - RC.CO-2 NIST Cybersecurity Framework v1.1 - RC.CO-3 NIST SP 800-53 R4 TR-3a[P]{0} NIST SP 800-53 r5 - PM-20 NY OHIP Moderate-Plus Security Baseline v5.0 - IA-8[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-20[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-20a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-20b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-20c

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization requires that PII, as well as software and services that receive, process, store, or transmit PII must be isolated within a service provider environment to the maximum extent possible so that the other service provider customers sharing physical or virtual space cannot gain access to such data or applications.

Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation (example):	The organization provides secure customer access to financial services, and develops and maintains policies and procedures to securely offer and ensure the resilience of remote financial services (e.g., using appropriate authentication, layered security controls, and fraud detection monitoring) in accordance with Appendix E of the FFIEC IT Handbook “Retail Payment Systems” booklet. The organization implements a customer awareness and education program that addresses both retail (consumer) and commercial account holders that includes the following elements: An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts accessible online; An explanation that while the institution may contact a customer regarding his or her account or suspicious activities related to his or her account, the institution never asks the customer to provide his or her log-in credentials over the phone or via e-mail; A list of recommended controls and prudent practices that the customer implements when using the institutions remote financial services; A suggestion that commercial online customers perform a related risk assessment and controls evaluation periodically; Recommendations of technical and business controls to commercial customers that can be implemented to mitigate the risks from fraud schemes such as Business Email Compromise; and A method to contact the institution if customers notice suspicious account activity.

Level FTI Custodians Implementation Requirements	

Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	The organization permits an individual to request to restrict the disclosure of the individual’s covered information to a business associate for purposes of carrying out payment or healthcare operations, and is not for purposes of carrying out treatment. The organization responds to any requests from an individual on the disclosure of the individual’s covered information, providing the individual with records of disclosures of covered information that are made by the organization; and either: records of disclosures of covered information made by a business associate acting on behalf of the organization; or, a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).

Control Reference: 05.k Addressing Security in Third Party Agreements

Control Specification:	Agreements with third-parties involving accessing, processing, communicating or managing the organization’s information or information assets, or adding products or services to information assets shall cover all relevant security requirements.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information
Level 1 Implementation (example):	The organization identifies and mandates information security controls to specifically address supplier access to the organization's information and information assets.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC9.2 Banking Requirements - FFIEC IS v2016 A.3.3 EU GDPR Article 32(4) ISO/IEC 27002:2022 - 5(19) ISO/IEC 27002:2022 - 5(22) ISO/IEC 27799:2016 15.1.1 ISO/IEC 27799:2016 15.1.2 ISO/IEC 27799:2016 15.1.3 PCI DSS v3.2.1 12.8.5 PCI DSS v3.2.1 2.6 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(f)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) HITRUST De-ID Framework Banking Requirements PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information High Low Moderate Supplemental
Level 2 Implementation (example):	The standard agreement with third-parties includes: the information security policy; procedures to protect organizational assets, including information, software, and hardware; any required physical protection controls and mechanisms; controls to ensure protection against malicious software; procedures to determine whether any compromise of the assets (e.g., loss or modification of information, software and hardware) has occurred; controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the agreement; confidentiality, integrity, availability, and any other relevant property of the assets; restrictions on copying and disclosing information, and using confidentiality agreements; user and administrator training in methods, procedures, and security; ensuring user awareness for information security responsibilities and issues; provision for the transfer of personnel, where appropriate; responsibilities regarding hardware and software installation and maintenance; a clear reporting structure and agreed reporting formats; a clear and specified process of change management; the different reasons, requirements, and benefits that make the access by the third party necessary; permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; an authorization process for user access and privileges; a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use; a statement that all access that is not explicitly authorized is forbidden; a process for revoking access rights or interrupting the connection between systems.

	The standard agreement with third-parties states: that the third party, following the discovery of a breach of unsecured covered information, notifies the organization of such breach, including the identification of each individual whose unsecured PII has been, or is reasonably believed by the third party to have been, accessed, acquired, or disclosed during such breach; that all security incident and breach-related notifications are made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach if the third party is an agent of the organization, otherwise the timing of the notification is explicitly addressed in the contract if the third party is not an agent of the organization; that evidence is maintained demonstrating that all security incident and breach-related notifications were made without unreasonable delay; that any other information that may be needed in the security incident and breach-related notification to individuals, either at the time notice of the breach is provided or promptly thereafter as information becomes available. The standard agreement with third-parties includes: a description of the product or service to be provided, and a description of the information to be made available along with its security classification; the target level of service and unacceptable levels of service; the definition of verifiable performance criteria, their monitoring and reporting; the right to monitor, and revoke, any activity related to the organization's assets; the right to audit responsibilities, defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors; the penalties exacted in the event of any failure in respect of the above; the establishment of an escalation process for problem resolution; service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities; the respective liabilities of the parties to the agreement; responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation) especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries; intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work; conditions for renegotiation/termination of agreements, including a contingency plan in place in case either party wishes to terminate the relation before the end of the agreements; conditions for renegotiation/termination of agreements, including renegotiation of agreements if the security requirements of the organization change; conditions for renegotiation/termination of agreements, including current documentation of asset lists, licenses, agreements, or rights relating to them. The organization requires third-party providers to notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within 15 calendar days.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.4 AICPA Trust Services Criteria - AICPA 2017 CC9.2 AICPA Trust Services Criteria - AICPA 2017 P6.1 AICPA Trust Services Criteria - AICPA 2017 P6.4 AICPA Trust Services Criteria - AICPA 2017 P6.5 Banking Requirements - FFIEC IS v2016 A.3.3 Banking Requirements - FFIEC IS v2016 A.6.31(c) Banking Requirements - FFIEC IS v2016 A.6.31(e) Banking Requirements - FFIEC IS v2016 A.6.31(f) Banking Requirements - FFIEC IS v2016 A.6.31(g) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) EU GDPR Article 32(4) FedRAMP - PS-7a[H] FedRAMP - PS-7a[L] FedRAMP - PS-7a[M] FedRAMP - PS-7c[H] FedRAMP - PS-7c[L] FedRAMP - PS-7c[M] Health Industry Cybersecurity Practices - 9.L.C HIPAA Privacy Rule - 164.504(e)(2)(i)(B) HIPAA Security Rule - § 164.314(a)(1) HIPAA Security Rule - § 164.314(a)(2)(i)(A) HIPAA Security Rule - § 164.314(a)(2)(i)(B) HIPAA Security Rule - § 164.314(a)(2)(i)(C) HIPAA Security Rule - § 164.314(a)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Third-party Assurance: General IRS Pub 1075 - 2.C.9(1)h IRS Pub 1075 - PS-7a IRS Pub 1075 - PS-7c ISO/IEC 27002:2022 - 5(21) ISO/IEC 27799:2016 15.1.1 ISO/IEC 27799:2016 15.1.2 ISO/IEC 27799:2016 15.1.3 ISO/IEC 27799:2016 7.1.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PS-7a MARS-E v2.2 - PS-7b MARS-E v2.2 - PS-7c NIST Cybersecurity Framework v1.1 - DE.CM-6 NIST Cybersecurity Framework v1.1 - ID.SC-3 NIST Cybersecurity Framework v1.1 - ID.SC-4 NIST Cybersecurity Framework v1.1 - PR.AT-3 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST SP 800-53 R4 PS-6a[HML]{2} NIST SP 800-53 R4 PS-7a[HML]{0} NIST SP 800-53 R4 PS-7c[HML]{0} NIST SP 800-53 R4 SA-10(4)[S]{2} NIST SP 800-53 R4 SA-10(5)[S]{2} NIST SP 800-53 R4 SA-10(6)[S]{3} NIST SP 800-53 r5 - PS-6a NIST SP 800-53 r5 - PS-7a NIST SP 800-53 r5 - PS-7b NIST SP 800-53 r5 - PS-7c NIST SP 800-53 r5 - SA-10(4) NIST SP 800-53 r5 - SA-10(5) NIST SP 800-53 r5 - SA-10(6)

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - SR-3(3) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-6(3) NY OHIP Moderate-Plus Security Baseline v5.0 - IR-6(3)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PS-7a NY OHIP Moderate-Plus Security Baseline v5.0 - PS-7b NY OHIP Moderate-Plus Security Baseline v5.0 - PS-7c NY OHIP Moderate-Plus Security Baseline v5.0 - SR-8 NY OHIP Moderate-Plus Security Baseline v5.0 - SR-8[IS.1] PCI DSS v3.2.1 12.8.2 PCI DSS v3.2.1 12.8.5 PCI DSS v3.2.1 12.9 PCI DSS v3.2.1 2.6 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(f) State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.210.3

Level Cloud Service Providers Implementation Requirements

Level Cloud Service Providers Implementation (example):	The organization ensures that mutually-agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development, information exchange, usage, and integrity persistence. Supply chain agreements (e.g., SLAs) between cloud service providers and customers (tenants) incorporate at least the following mutually-agreed upon provisions and/or terms: Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations); Information security requirements; Provider and customer (tenant) primary points of contact for the duration of the business relationship; References to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships; Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts; Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain); Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed; Expiration of the business relationship and treatment of customer (tenant) data impacted; and Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	The organization ensures acquisition contracts contain appropriate language from IRS Pub 1075, Safeguarding Contract Language. Organization-defined security and privacy controls for third-party arrangements (e.g., in cloud service providers) are identified, documented (e.g., in a legally-binding contract or SLA), and implemented. The defined security and privacy controls, as implemented, must comply with the requirements specified in IRS Pub 1075.

	The organization must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or Service Level Agreement (SLA) with its third-party cloud provider. Additional SLA requirements include but are not limited to: FTI must be encrypted in transit within the cloud environment, all mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module; FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud–if the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control; and storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS).
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	If the organization is classified as a joint controller, the controller jointly determines: the purposes and means of processing with one or more other controllers; with one or more other controllers their respective responsibilities for compliance with their obligations under GDPR in a transparent manner; with one or more other controllers their respective responsibilities with respect to the exercising of the rights of the data subject whether obtained by the controller from the subject or from another source, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by EU or Member State law to which the controllers are subject; and with one or more other controllers their respective responsibilities with respect to their respective duties to provide information regarding access to personal data whether obtained by the controller from the subject or from another source, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by EU or Member State law to which the controllers are subject. This arrangement duly reflects the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement is made available to the data subject. Each data controller involved in the arrangement specifically allows a data subject to exercise the subjects rights under the GDPR in respect of and against each of the controllers. The processor only engages with another processer when given prior specific or general written authorization of the controller. In the case of general written authorization–the processor informs the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
Level HIE Implementation Requirements	
Level HIE Implementation (example):	As part of the agreement with the connecting organizations, the HIE specifies: the requirements of the connecting organization to define and communicate to the HIE access roles for the connecting organization's employees; that it is the sole responsibility of the connecting organization to appropriately restrict access in accordance with federal and state requirements (e.g., mental health information); and the requirements of connecting organizations to request and receive detailed access logs related to the connecting organization's records.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization identifies and documents information about which PCI DSS requirements are managed by each service provider, and which are managed by the organization.

Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	Supplier complies to requirements under the supplier agreement, including maintaining and adhering to documented processes for: reviewing and scanning software developed or customized for the organization to find and remediate malicious code and/or security vulnerabilities prior to initial deployment, and making scan results and remediation plans available to the organization upon request; cooperating with the organization and taking all reasonable and necessary steps to isolate, mitigate, terminate, and/or remediate all known or suspected threats within 90 days of notification of a threat to the organization or its customers' nonpublic information resources originating from the supplier's network; and notifying and cooperating with the organization upon discovery of a supplier's noncompliance with the organization's security requirements, or of a known or suspected threat/vulnerability impacting the organization or its customers, and to take all reasonable and necessary steps to isolate, mitigate, and/or remediate such noncompliance or threat/vulnerability within 90 days. Supplier maintains and adheres to any business continuity plan and/or disaster recovery plan requirements under the agreement.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization executes service contracts for incident management through an outside legal party to ensure client/attorney confidentiality.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	Data is removed from the contractor's system and returned to the organization within the timeframe stipulated by the contractual agreement and/or organization policy.

Control Category: 06.0 - Compliance

Objective Name: 06.01 Compliance with Legal Requirements

Control Objective:	To ensure that the design, operation, use, and management of information systems adheres to applicable laws, statutory, regulatory or contractual obligations, and any security requirements.
Control Reference: 06.a Identification of Applicable Legislation	
Control Specification:	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	

Level 1 Regulatory Factors:	DirectTrust FTC Red Flags Rule (16 CFR 681) State of Massachusetts Data Protection Act (201 CMR 17.00)
Level 1 Implementation (example):	All relevant statutory, regulatory, and contractual requirements, including the specific controls and individual responsibilities to meet these requirements, are explicitly defined and formally documented (e.g., in policies and procedures, as appropriate) for each information system type, and communicated to the user community as necessary through documented security training and awareness programs.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(B)(xviii)(I) 23 NYCRR 500 - 500.02(b)(6) Banking Requirements - FFIEC IS v2016 A.4.5 FTC Red Flags Rule (16 CFR 681) - 681.A7.a FTC Red Flags Rule (16 CFR 681) - 681.A7.b FTC Red Flags Rule (16 CFR 681) - 681.A7.c FTC Red Flags Rule (16 CFR 681) - 681.A7.d Health Industry Cybersecurity Practices - 10.M.A HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) ISO/IEC 27002:2022 - 5(31) ISO/IEC 27002:2022 - 5(4) ISO/IEC 27002:2022 - 5(5) ISO/IEC 27799:2016 18.1.1 ISO/IEC 27799:2016 7.2.2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(1) State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.215.1 Veterans Affairs Cybersecurity Program Directive 6500 - a(1)(e) Veterans Affairs Cybersecurity Program Directive 6500 - a(3)(g) Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(b) Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(c) Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(e) Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(g) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(d) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(c) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(k) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(l)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Banking Requirements

Level 2 Implementation (example):	The organization joins industry trade associations, subscribes to thought leadership and market/security research organizations, or establishes some other reliable process to stay abreast of business sector, industry, technology, infrastructure, legal, and regulatory environment trends that may impact the organization's security policies. Consequences of business sector, industry, technology, infrastructure, legal and regulatory environment trends impacting the organizations security policies are incorporated into the development or update of IT policies and procedures.
Level 2 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC1.3 Banking Requirements - FFIEC IS v2016 A.4.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-15 (HIGH; MOD) Health Industry Cybersecurity Practices - 8.S.B HIPAA Privacy Rule - 164.530(i)(2)(i) HIPAA Privacy Rule - 164.530(i)(2)(iii) HIPAA Privacy Rule - 164.530(i)(4)(i)(A) HIPAA Privacy Rule - 164.530(i)(4)(i)(B) HIPAA Privacy Rule - 164.530(i)(5)(i) ISO/IEC 27799:2016 18.1.1 ISO/IEC 27799:2016 6.1.4 NIST Cybersecurity Framework v1.1 - ID.RA-4 NIST Cybersecurity Framework v1.1 - PR.IP-7 NIST Cybersecurity Framework v1.1 - RS.CO-5 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-15c

Control Reference: 06.b Intellectual Property Rights

Control Specification:	Detailed procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights, and on the use of proprietary software products.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP Supplemental
Level 1 Implementation (example):	The organization establishes restrictions on the use of open source software. Open source software used by the organization is legally licensed, authorized, and adheres to the organizations secure configuration policy.

Level 1 Authoritative Source Mapping:	FedRAMP - CM-10(1)[H] FedRAMP - CM-10(1)[M] FedRAMP - SI-7(14)a[H] FedRAMP - SI-7(14)b[H] MARS-E v2.2 - CM-10(1) MARS-E v2.2 - CM-7(2)a MARS-E v2.2 - CM-7(2)b MARS-E v2.2 - CM-7(2)c NIST SP 800-53 R4 CM-10(1)[S]{0} NIST SP 800-53 r5 - CM-10(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-10(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	High Low Moderate Supplemental
Level 2 Implementation (example):	The organization ensures compliance with any legislative, regulatory, or contractual requirements that may place restrictions on the copying of proprietary material including copyrights, design rights, or trademarks by: acquiring software only through known and reputable sources, to ensure that copyright is not violated; maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.; implementing controls to ensure that any maximum number of users permitted is not exceeded; carrying out annual checks that only authorized software and licensed products are installed; developing and providing a policy for maintaining agreed upon license conditions; using manual audit tools; complying with terms and conditions for software and information obtained from public networks; and use of proprietary software must also be in compliance with encryption, export and local data privacy regulations. The organization ensures compliance with any legislative, regulatory, or contractual requirements that may place restrictions on the copying of proprietary material including copyrights, design rights, or trademarks by also: publishing an intellectual property rights compliance policy which defines the legal use of software and information products; maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them; maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights; developing and providing a policy for disposing or transferring software to others; not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Level 2 Authoritative Source Mapping:	FedRAMP - CM-10a[H] FedRAMP - CM-10a[L] FedRAMP - CM-10a[M] FedRAMP - CM-10b[H] FedRAMP - CM-10b[L] FedRAMP - CM-10b[M] IRS Pub 1075 - CM-10a IRS Pub 1075 - CM-10b ISO/IEC 27002:2022 - 5(32) ISO/IEC 27799:2016 18.1.2 MARS-E v2.2 - CM-10a MARS-E v2.2 - CM-10b NIST Cybersecurity Framework v1.1 - ID.GV-3 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 R4 CM-10b[HML]{0} NIST SP 800-53 R4 SI-12[HML]{4} NIST SP 800-53 R4 SI-14(1)[S]{2} NIST SP 800-53 r5 - CM-10b NIST SP 800-53 r5 - SI-14(1) NIST SP 800-53 r5 - SR-5 NY OHIP Moderate-Plus Security Baseline v5.0 - CM-10a NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(2)a NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(2)c
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High) High Low Moderate
Level 3 Implementation (example):	The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Software license tracking is accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational need.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-10 (HIGH; MOD) FedRAMP - CM-10c[H] FedRAMP - CM-10c[L] FedRAMP - CM-10c[M] IRS Pub 1075 - CM-10c MARS-E v2.2 - CM-10c NIST SP 800-53 R4 CM-10c[HML]{0} NIST SP 800-53 r5 - CM-10c NY OHIP Moderate-Plus Security Baseline v5.0 - CM-10b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-10c

Level FedRAMP Implementation Requirements

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	The organization establishes restrictions on the use of open source software. Any open source software used by the organization is legally licensed, approved by the organization's IT department, and adheres to a secure configuration baseline checklist from the U.S. Government or industry.

Control Reference: 06.c Protection of Organizational Records

Control Specification:	Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust The Joint Commission v2016 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements State of Nevada Security and Privacy of Personal Information
Level 1 Implementation (example):	Guidelines are issued and implemented by the organization on the ownership, classification, retention, storage, handling, and disposal of all records and information.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(c) 21 CFR Part 11.30 AICPA Trust Services Criteria - AICPA 2017 C1.1 AICPA Trust Services Criteria - AICPA 2017 C1.2 Banking Requirements - FFIEC IS v2016 A.6.18(a) FTC Red Flags Rule (16 CFR 681) - 681.2c1.i FTC Red Flags Rule (16 CFR 681) - 681.2c2 Health Industry Cybersecurity Practices - 10.M.A Health Industry Cybersecurity Practices - 4.M.B Health Industry Cybersecurity Practices - 4.M.C Health Industry Cybersecurity Practices - 4.S.A Health Industry Cybersecurity Practices - 4.S.B Health Industry Cybersecurity Practices - 5.M.C Health Industry Cybersecurity Practices - 5.M.D Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.310(d)(2)(i) HIPAA Security Rule - § 164.310(d)(2)(ii) HIPAA Security Rule - § 164.316(b)(1)(ii) ISO/IEC 27001:2022 - 7.5.3d ISO/IEC 27001:2022 - 7.5.3e ISO/IEC 27001:2022 - 7.5.3f ISO/IEC 27002:2022 - 5(10) ISO/IEC 27799:2016 18.1.3 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(g) The Joint Commission (v2016) - TJC IM.02.01.03, EP 6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	DirectTrust EHNAC FedRAMP FISMA HITRUST De-ID Framework The Joint Commission v2016 Banking Requirements PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information High Low Moderate Privacy Supplemental
Level 2 Implementation (example):	The organization's formal policies, formal procedures, other critical records (e.g., results from a risk assessment), and disclosures of individuals' protected health information are retained for a minimum of six years. For electronic health records, the organization must retain records of disclosures to carry out treatment, payment and healthcare operations for a minimum of three years. The organization documents and maintains: accountings of disclosure as organizational records for a period of six years; the information required for disclosure; the written accounting provided to the individual; the titles of the persons or offices responsible for receiving and processing requests for an accounting.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(c) 21 CFR Part 11.30 AICPA Trust Services Criteria - AICPA 2017 C1.1 AICPA Trust Services Criteria - AICPA 2017 C1.2 AICPA Trust Services Criteria - AICPA 2017 P4.2 Banking Requirements - FFIEC IS v2016 A.6.18(a) Banking Requirements - FFIEC IS v2016 A.6.18(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-02(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-12 (HIGH; MOD) HIPAA Breach Notification Rule - 164.414(a) HIPAA Privacy Rule - 164.504(e)(2)(ii)(B) HIPAA Privacy Rule - 164.504(e)(2)(ii)(G) HIPAA Privacy Rule - 164.504(f)(2)(ii)(G) HIPAA Privacy Rule - 164.524(e)(2) HIPAA Privacy Rule - 164.528(a)(1)(i) HIPAA Privacy Rule - 164.528(a)(1)(ii) HIPAA Privacy Rule - 164.528(a)(1)(iii) HIPAA Privacy Rule - 164.528(a)(1)(iv) HIPAA Privacy Rule - 164.528(a)(1)(ix) HIPAA Privacy Rule - 164.528(a)(3) HIPAA Privacy Rule - 164.528(b)(1) HIPAA Privacy Rule - 164.528(b)(2)(i) HIPAA Privacy Rule - 164.528(b)(2)(ii) HIPAA Privacy Rule - 164.528(b)(3)(i) HIPAA Privacy Rule - 164.528(b)(3)(ii) HIPAA Privacy Rule - 164.528(b)(4)(i)(A) HIPAA Privacy Rule - 164.528(b)(4)(i)(B) HIPAA Privacy Rule - 164.528(b)(4)(i)(C) HIPAA Privacy Rule - 164.528(b)(4)(i)(D) HIPAA Privacy Rule - 164.528(b)(4)(i)(E) HIPAA Privacy Rule - 164.528(b)(4)(i)(F) HIPAA Privacy Rule - 164.528(b)(4)(ii) HIPAA Privacy Rule - 164.528(d)(1) HIPAA Privacy Rule - 164.528(d)(2) HIPAA Privacy Rule - 164.528(d)(3) HIPAA Privacy Rule - 164.530(i)(5)(ii) HIPAA Privacy Rule - 164.530(j)(1)(i) HIPAA Privacy Rule - 164.530(j)(1)(ii) HIPAA Privacy Rule - 164.530(j)(1)(iii) HIPAA Privacy Rule - 164.530(j)(1)(iv) HIPAA Privacy Rule - 164.530(j)(2) HIPAA Security Rule - § 164.308(a)(2) HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.310(d)(2)(i) HIPAA Security Rule - § 164.310(d)(2)(iv) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(e)(2)(i) HIPAA Security Rule - § 164.312(e)(2)(ii) HIPAA Security Rule - § 164.316(b)(1)(ii) HIPAA Security Rule - § 164.316(b)(2)(i) HITRUST De-ID Framework - De-ID Framework v1 Retention: Data Retention Policy ISO/IEC 27002:2022 - 5(33) ISO/IEC 27799:2016 18.1.3

Level 2 Authoritative Source Mapping (Cont.):	ISO/IEC 27799:2016 8.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PL-1a1 MARS-E v2.2 - PL-2a1 NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST Cybersecurity Framework v1.1 - PR.IP-4 NIST Cybersecurity Framework v1.1 - PR.IP-6 NIST SP 800-53 R4 AC-16(2)[S]{2} NIST SP 800-53 R4 AU-11(1)[S]{1} NIST SP 800-53 R4 CP-9(7)[S]{0} NIST SP 800-53 R4 CP-9[HML]{4} NIST SP 800-53 R4 DM-2c[P]{0} NIST SP 800-53 R4 RA-2c[HML]{0} NIST SP 800-53 R4 SI-12[HML]{1} NIST SP 800-53 r5 - AC-16(2) NIST SP 800-53 r5 - AU-11(1) NIST SP 800-53 r5 - CP-9 NIST SP 800-53 r5 - CP-9(7) NIST SP 800-53 r5 - RA-2c NIST SP 800-53 r5 - SI-14(2) NIST SP 800-53 r5 - SI-21 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(7)[NYS.4] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-1[PHI.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-2[PHI.1] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-2[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-2[PHI.1] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-2c PCI DSS v3.2.1 3.1 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(g) The Joint Commission (v2016) - TJC IM.02.01.03, EP 6 Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(c)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization retains output, including but not limited to audit records, system records, business and financial reports, and business records from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization identifies unauthorized use of the information system through organization-defined techniques and methods.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Audit information is archived for seven years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored, supports after-the-fact investigations of security incidents, and meets regulatory and organization information retention requirements. The organization provides an explicit indication of current participants in meetings that involve FTI.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization retains output, including but not limited to audit records, system records, business and financial reports, and business records from the information system for ten years or in accordance with Administering Entity organizational requirements.

Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization keeps cardholder data storage to a minimum by implementing specific data retention and disposal policies, procedures, and processes for all cardholder data (CHD) storage.
Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	Guidelines are issued by the organization on the ownership, classification, retention, storage, handling, return and disposal of all records and information. Separation between operational information and non-production (development, test/quality assurance) environments is maintained.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	The organization documents compliance with the notice requirements by retaining copies of the notices issued by the organization for a period of six years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement. The organization documents restrictions in writing and formally maintain such writing, or an electronic copy of such writing, as an organizational record for a period of six years.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system implements cryptographic mechanisms, in transit and at rest, as defined in the HHS Standard for Encryption of Computing Devices and Information, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The information system protects the confidentiality and integrity of information at rest, as defined in the HHS Standard for Encryption of Computing Devices and Information.

Control Reference: 06.d Data Protection and Privacy of Covered Information

Control Specification:	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and contractual clauses.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Community Supplemental Requirements 002 DirectTrust The Joint Commission v2016 CA Civil Code § 1798.81.5 Supplemental Requirements Texas Medical Records Privacy Act State of Nevada Security and Privacy of Personal Information

Level 1 Implementation (example):	Covered and/or confidential information, at minimum, is rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs. Exceptions to encryption requirements are authorized by management and documented. Encryption is implemented via one-way hashes, truncation, or strong cryptography and key-management procedures. For full-disk encryption, logical access is independent of O/S access. Decryption keys are not tied to user accounts. If encryption is not applied because it is determined to not be reasonable or appropriate, the organization documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.30 AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.30 CIS Controls v7.1 - CIS CSC v7.1 14.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-12(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-28 (HIGH; MOD) Community Supplemental Requirements 002 - CSR002 v2018 11.2-6-0 Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(e)(2)(ii) HITRUST ISO/IEC 27799:2016 18.1.4 MARS-E v2.2 - SC-28a NIST Cybersecurity Framework v1.1 - PR.DS-1 NIST SP 800-171 r2 - 3.13.16[a] OCR Guidance for Unsecured PHI (1)(i) OCR Guidance for Unsecured PHI (1)(ii) PCI DSS v3.2.1 3.4 The Joint Commission (v2016) - TJC IM.02.01.03, EP 2
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA HITRUST De-ID Framework The Joint Commission v2016 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information
Level 2 Implementation (example):	There is an appointment of a person responsible, such as a data protection officer or privacy officer, who reports directly to the highest level of management in the organization (e.g., a CEO), and is responsible for the organization's individual privacy protection program. Such appointment is based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill required tasks. Responsibilities include the development and implementation of privacy policies and procedures, serving as the point of contact for all privacy-related issues, including the receipt of privacy-related complaints, and providing privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that are followed. The data protection officer will, in the performance of those tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context, and purposes of processing, and may fulfill other tasks and duties; however, the organization ensures that any such tasks and duties do not result in a conflict of interests. The organization supports the data protection officer in performing the tasks required by law or regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain the data protection officers expert knowledge, and ensures that the data protection or privacy officer does not receive any instructions regarding the exercise of those tasks, and the officer is bound by secrecy or confidentiality concerning the performance of those tasks, in accordance with applicable law or regulation. The officer is not to be dismissed or penalized by the organization for performing those tasks. Where required by legislation, consent is obtained before any PII (e.g., about a client/customer) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(i) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xv) 21 CFR Part 11.30 Banking Requirements - FFIEC IS v2016 A.6.18(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-12 (HIGH) EU GDPR Article 37(1) EU GDPR Article 37(2) EU GDPR Article 37(5) EU GDPR Article 38(1) EU GDPR Article 38(2) EU GDPR Article 38(3) EU GDPR Article 39(1) EU GDPR Article 39(2) HIPAA Privacy Rule - 164.504(e)(2)(ii)(B) HIPAA Privacy Rule - 164.530(a)(1)(i) HIPAA Privacy Rule - 164.530(a)(2) HIPAA Privacy Rule - 164.532(c)(2) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.308(b)(1) HIPAA Security Rule - § 164.308(b)(2) HIPAA Security Rule - § 164.310(d)(2)(i) HITRUST De-ID Framework - De-ID Framework v1 Data Storage: General HITRUST De-ID Framework - De-ID Framework v1 Storage (Minimal Locations Authorized): Implementation HITRUST De-ID Framework - De-ID Framework v1 Storage (Minimal Locations Authorized): Policy ISO/IEC 27799:2016 18.1.3 ISO/IEC 27799:2016 18.1.4 ISO/IEC 27799:2016 7.12.2.2 Legacy Inheritance Support - L.I.S. NIST SP 800-53 r5 - AC-4(24) NIST SP 800-53 r5 - SA-8(33) NY OHIP Moderate-Plus Security Baseline v5.0 - SA-8(33) Ontario Personal Health Information Protection Act - 15(2) Ontario Personal Health Information Protection Act - 15(4) PCI DSS v3.2.1 3.1 The Joint Commission (v2016) - TJC IM.02.01.03, EP 2 Veterans Affairs Cybersecurity Program Directive 6500 - a(2)(b)
Level CIS Implementation Requirements	
Level CIS Implementation (example):	Access to encrypted information at rest requires a secondary authentication mechanism, not integrated into the operating system.
Level De-ID Data Environment Implementation Requirements	
Level De-ID Data Environment Implementation (example):	Encryption has been implemented for covered information in transit, whether internal or external, to the organization’s network. If encryption is not used for data in transit the organization has documented its rationale.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization is not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. The organization ensures that FTI will not be subject to public disclosure.

	FTI stored on deployed user workstations, in non-volatile storage, is encrypted with FIPS-validated or National Security Agency- (NSA-) approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The data controller or processor, which is not established in the EU, designates in writing a representative in the EU, in one of the EU member states where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored. A data protection officer is designated for a controller, processor, group of undertakings, provided the officer is accessible from each establishment, or group of multiple public authorities or bodies, taking account of their organizational structure and size, in any case where (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; OR (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law, also designates a data protection officer, who may act for such associations and other bodies representing controllers or processors. The controller or the processor requires publication of the contact details and communication of those details to the supervisory authority.
Level Group Health Plans Implementation Requirements	
Level Group Health Plans Implementation (example):	Group Health Plan documents require the plan sponsor to implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information (ePHI) created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan, except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to 45 CFR § 164.504(f)(1)(ii) or (iii), or as authorized under 45 CFR § 164.508. Group Health Plan documents require the plan sponsor to: ensure that adequate separation is supported by reasonable and appropriate security measures; ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and report to the group health plan any security incident of which it becomes aware.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization renders the Primary Account Number (PAN) unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography, (hash must be of the entire PAN); truncation (hashing cannot be used to replace the truncated segment of the PAN); index tokens and pads (pads must be securely stored); or, strong cryptography with associated key management processes and procedures. If disk encryption is used (rather than file- or column-level database encryption), logical access is managed separately and independently of native operating system authentication and access control mechanisms (e.g., by not using local user account databases or general network login credentials). Decryption keys are not associated with user accounts.

Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	Workstations that can access covered and/or confidential information are configured based on specifications that address: proper functions to be performed, the manner in which those functions are to be performed, and physical attributes of the surroundings.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization limits access to PII: from external information systems (including, but not limited to, personally owned information systems/devices); and to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements which protect the PII. The organization implements controls that include either full-device or virtual container encryption to reduce the vulnerability of PII contained on mobile devices.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization fragments organization-defined information (i.e., covered information) and distributes the fragmented information across the organization-defined systems or system components. The information system that transfers information between different security domains: does not filter message content; validates filtering metadata; ensures the content associated with the filtering of metadata has successfully completed filtering; and transfers the content to the destination filter pipeline.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The organization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of confidential state data at rest on system components that host confidential state data. The organization identifies and documents the location of organization-defined information and the specific system components on which the information is processed and stored, and documents changes to the location (i.e., system or system components) where the information is processed and stored.
Level VA Directive 6500 Implementation Requirements	
Level VA Directive 6500 Implementation (example):	The organization implements cryptography in accordance Federal Information Processing Standards (FIPS) 140-3 to protect VA information.

Control Reference: 06.e Prevention of Misuse of Information Assets

Control Specification:	Users shall be deterred from using information assets for unauthorized purposes.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	PCI DSS v3.2.1

Level 1 Implementation (example):	All employees and contractors are informed in writing that violations of the security policies will result in sanctions or disciplinary action.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.1 AICPA Trust Services Criteria - AICPA 2017 CC1.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) HIPAA Privacy Rule - 164.530(e)(1) HIPAA Privacy Rule - 164.530(e)(2) HIPAA Security Rule - § 164.308(a)(1)(ii)(C) IRS Pub 1075 - 2.D.2.1(3) IRS Pub 1075 - 2.D.2.1(5) ISO/IEC 27001:2022 - 7.3c MARS-E v2.2 - PL-4e NIST Cybersecurity Framework v1.1 - PR.IP-11 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-3(9)[NYS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4e

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	Communication to all employees has notified them that their actions to information assets may be monitored and through signing an acceptable use agreement they have consented to such monitoring as permitted by the applicable legal jurisdiction. The organization provides notice that the employee’s actions may be monitored, and the employee consents to such monitoring.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-08 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.310(b) HIPAA Security Rule - § 164.312(b) NIST SP 800-53 R4 PL-4b[HML]{2} NIST SP 800-53 r5 - PL-4b NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4f PCI DSS v3.2.1 12.3.1 Supplemental Requirements - SR v6.4 24-0

Level CMS Implementation Requirements

Level CMS Implementation (example):	The approved banner used for CMS information systems communicates that: you are accessing a U.S. Government information system which includes this computer; you are accessing a U.S. Government information system which includes this computer network; you are accessing a U.S. Government information system which includes all computers connected to this network; you are accessing a U.S. Government information system which includes all devices and storage media attached to this network or to a computer on this network–this information system is provided for U.S. Government-authorized use only; unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties; you understand and consent to the fact that you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system, at any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system; and you understand and consent to the fact that any communication or data transiting or stored on this information system may be disclosed or used for any lawful government purpose. For publicly accessible systems, the approved banner: displays the system use information when appropriate before granting further access; displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The service provider determines elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Joint Authorization Board (JAB). The service provider determines how System Use Notification is going to be verified and provides appropriate periodicity of the check. The System Use Notification verification is approved and accepted by the Joint Authorization Board (JAB). The check periodicity is approved and accepted by the Joint Authorization Board (JAB).

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	The warning banner for all FTI systems contains reference to the civil and criminal penalty sections of Title 26 Section 7213, 26 Section 7213A, and 26 Section 7431.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes this computer network, all computers connected to this network, and all devices and storage media attached to this network or to a computer on this network. The banner states that: the system is provided for Government authorized use only; unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties; personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring; and by using this system, you understand and consent to the following: “The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.”; “Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose”. The information system retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system. For publicly accessible systems, the information system: displays system use information when appropriate, before granting further access; displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and includes a description of the authorized uses of the system. Pursuant to OMB M-17-12, organizational rules of behavior include a policy outlining the: rules of behavior to safeguard personally identifiable information (PII); consequences for failure to follow these rules; and corrective actions for failure to follow these rules. Consequences are commensurate with level of responsibility and type of PII involved.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The information system displays to users organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The logon notification message/banner states that: users are accessing a U.S. Government information system; information system usage may be monitored, recorded, and subject to audit; unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and use of the information system indicates consent to monitoring and recording. The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system. For publicly accessible systems, the information system: displays system use information organization-defined conditions, before granting further access; displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and includes a description of the authorized uses of the system in the logon notification/banner. The information system displays an explicit logout message to users indicating the termination of authenticated communications sessions.

Control Reference: 06.f Regulation of Cryptographic Controls

Control Specification:	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The encryption policy addresses the type and strength of the encryption algorithm and when used to protect the confidentiality of information. The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.02(a) 23 NYCRR 500 - 500.11(b)(2) 23 NYCRR 500 - 500.15(a)(1) 23 NYCRR 500 - 500.15(a)(2) 23 NYCRR 500 - 500.15(b) Health Industry Cybersecurity Practices - 1.M.C Health Industry Cybersecurity Practices - 10.M.A ISO/IEC 27002:2022 - 8(24) NIST SP 800-171 r2 - 3.13.11[a]

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The organization ensures legal advice is sought in relation to all relevant regulations governing the use of cryptographic controls by the organization. Compliance with all relevant regulations governing the use of cryptographic controls is reviewed on an annual basis at a minimum.

	The organization accounts for any country specific regulations governing the use of cryptographic controls including: import and/or export of computer hardware and software for performing cryptographic functions; import and/or export of computer hardware and software which is designed to have cryptographic functions added to it; restrictions on the usage of encryption; mandatory or discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content; and mechanisms for authentication to a cryptographic module that meets U.S. requirements for such authentication (e.g., validation under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2), if applicable. Legal advice is specific to either the country where the cryptographic controls are used, or the country to which such controls are imported or exported.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-13 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) ISO/IEC 27799:2016 18.1.1 ISO/IEC 27799:2016 18.1.2 ISO/IEC 27799:2016 18.1.5 NIST Cybersecurity Framework v1.1 - ID.GV-3
Level CMS Implementation Requirements	
Level CMS Implementation (example):	When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization determines the cryptographic uses and implements the cryptography required for each specified cryptographic use (e.g., Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, encryption in transit). The organization accepts only external authenticators that are NIST-compliant, and documents and maintains a list of accepted external authenticators.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization uses a defined encryption methodology to encrypt personally identifiable information (PII) confidentiality impact level in backups at the storage location. The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Objective Name: 06.02 Compliance with Security Policies and Standards, and Technical Compliance

Control Objective:	To ensure that the design, operation, use and management of information systems adheres to organizational security policies and standards.

Control Reference: 06.g Compliance with Security Policies and Standards	
Control Specification:	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	The Joint Commission v2016 Texas Medical Records Privacy Act
Level 1 Implementation (example):	Annual compliance assessments are conducted. Compliance reviews are conducted by security, privacy, and/or audit individuals, and incorporate reviews of documented evidence. If any non-compliance is found as a result of the review, managers will: determine the causes of the non-compliance; evaluate the need for actions to ensure that non-compliance do not recur; determine and implement appropriate corrective action; and review the corrective action taken.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC2.1 Banking Requirements - FFIEC IS v2016 A.10.1 Banking Requirements - FFIEC IS v2016 A.10.3(a) Banking Requirements - FFIEC IS v2016 A.6.4(c) Banking Requirements - FFIEC IS v2016 A.8.1(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 FTC Red Flags Rule (16 CFR 681) - 681.A6.b1 FTC Red Flags Rule (16 CFR 681) - 681.A6.b2 HIPAA Security Rule - § 164.308(a)(8) ISO/IEC 27001:2022 - 10.2d ISO/IEC 27001:2022 - 10.2e ISO/IEC 27001:2022 - 9.2.2e ISO/IEC 27001:2022 - 9.3.2a ISO/IEC 27002:2022 - 5(36) ISO/IEC 27799:2016 18.2.2 ISO/IEC 27799:2016 18.2.3 MARS-E v2.2 - AR-4a MARS-E v2.2 - AR-4c The Joint Commission (v2016) - TJC IM.02.01.03, EP 8

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA The Joint Commission v2016 Banking Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The results and recommendations of the compliance reviews are documented, and approved by management. Automated compliance tools/scans are used where possible.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.10.1 Banking Requirements - FFIEC IS v2016 A.10.3(a) Banking Requirements - FFIEC IS v2016 A.10.5 Banking Requirements - FFIEC IS v2016 A.10.6 Banking Requirements - FFIEC IS v2016 A.4.1 Banking Requirements - FFIEC IS v2016 A.7.4(c) Banking Requirements - FFIEC IS v2016 A.7.4(d) Banking Requirements - FFIEC IS v2016 A.8.1(c) Banking Requirements - FFIEC IS v2016 A.8.1(o) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-07(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 FedRAMP - CA-2(1)[H] FedRAMP - CA-2(1)[L] FedRAMP - CA-2(1)[M] FedRAMP - CA-7(1)[H] FedRAMP - CA-7(1)[M] FedRAMP - CA-7(3)[H] FedRAMP - CA-7a[H] FedRAMP - CA-7a[L] FedRAMP - CA-7a[M] FedRAMP - CA-7b[H] FedRAMP - CA-7b[L] FedRAMP - CA-7b[M] FedRAMP - CA-7c[H] FedRAMP - CA-7c[L] FedRAMP - CA-7c[M] FedRAMP - CA-7d[H] FedRAMP - CA-7d[L] FedRAMP - CA-7d[M] FedRAMP - CA-7e[H] FedRAMP - CA-7e[L] FedRAMP - CA-7e[M] FedRAMP - CA-7f[H] FedRAMP - CA-7f[L] FedRAMP - CA-7f[M] FedRAMP - CA-7g[H] FedRAMP - CA-7g[L] FedRAMP - CA-7g[M] FedRAMP - PS-7e[H] FedRAMP - PS-7e[L] FedRAMP - PS-7e[M] FTC Red Flags Rule (16 CFR 681) - 681.A6.a2 Health Industry Cybersecurity Practices - 1.L.C HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(8) HIPAA Security Rule - § 164.312(b) IRS Pub 1075 - CA-2(1) IRS Pub 1075 - CA-7(1) IRS Pub 1075 - CA-7(4)a IRS Pub 1075 - CA-7(4)b IRS Pub 1075 - CA-7(4)c IRS Pub 1075 - CA-7a

Level 2 Authoritative Source Mapping (Cont.):	IRS Pub 1075 - CA-7b IRS Pub 1075 - CA-7d IRS Pub 1075 - CA-7e IRS Pub 1075 - CA-7f IRS Pub 1075 - CA-7g IRS Pub 1075 - PS-7e ISO/IEC 27001:2022 - 6.2b ISO/IEC 27001:2022 - 6.2d ISO/IEC 27001:2022 - 8.2b ISO/IEC 27001:2022 - 8.3b ISO/IEC 27001:2022 - 9.1a ISO/IEC 27001:2022 - 9.1b ISO/IEC 27001:2022 - 9.1c ISO/IEC 27001:2022 - 9.1d ISO/IEC 27001:2022 - 9.1e ISO/IEC 27001:2022 - 9.1f ISO/IEC 27001:2022 - 9.1g ISO/IEC 27001:2022 - 9.1h ISO/IEC 27001:2022 - 9.2.1a1 ISO/IEC 27001:2022 - 9.2.1a2 ISO/IEC 27001:2022 - 9.2.1b ISO/IEC 27001:2022 - 9.2.2a ISO/IEC 27001:2022 - 9.2.2b ISO/IEC 27001:2022 - 9.2.2c ISO/IEC 27001:2022 - 9.2.2d ISO/IEC 27001:2022 - 9.3.2d2 ISO/IEC 27001:2022 - 9.3.2d3 ISO/IEC 27001:2022 - 9.3.3b ISO/IEC 27002:2022 - 8(16) ISO/IEC 27002:2022 - 8(34) ISO/IEC 27799:2016 12.7.1 ISO/IEC 27799:2016 18.2.2 ISO/IEC 27799:2016 18.2.3 MARS-E v2.2 - CA-7a MARS-E v2.2 - CA-7d MARS-E v2.2 - CA-7e MARS-E v2.2 - CA-7f MARS-E v2.2 - CA-7g MARS-E v2.2 - CA-7h NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - DE.DP-2 NIST Cybersecurity Framework v1.1 - DE.DP-4 NIST Cybersecurity Framework v1.1 - ID.GV-4 NIST Cybersecurity Framework v1.1 - ID.RA-4 NIST Cybersecurity Framework v1.1 - ID.RM-1 NIST SP 800-53 R4 CA-2(1)[HM]{0} NIST SP 800-53 R4 CA-7(1)[HM]{0} NIST SP 800-53 R4 CA-7(3)[S]{0} NIST SP 800-53 R4 CA-7[HML]{0} NIST SP 800-53 R4 PS-7e[HML]{0} NIST SP 800-53 r5 - CA-2(1) NIST SP 800-53 r5 - CA-2a NIST SP 800-53 r5 - CA-7(1) NIST SP 800-53 r5 - CA-7(3) NIST SP 800-53 r5 - CA-7(4)b NIST SP 800-53 r5 - CA-7a NIST SP 800-53 r5 - PM-31 NIST SP 800-53 r5 - RA-3b NIST SP 800-53 r5 - RA-7 NY OHIP Moderate-Plus Security Baseline v5.0 - CA-2a

Level 2 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - CA-7[IS.1e] NY OHIP Moderate-Plus Security Baseline v5.0 - CA-7[IS.1f] NY OHIP Moderate-Plus Security Baseline v5.0 - CA-7e NY OHIP Moderate-Plus Security Baseline v5.0 - CA-7f NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-31[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-31a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-31c NY OHIP Moderate-Plus Security Baseline v5.0 - PM-31d NY OHIP Moderate-Plus Security Baseline v5.0 - PM-31e NY OHIP Moderate-Plus Security Baseline v5.0 - PM-31f Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(c)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs assessors or assessment teams with CMS CISO defined level of independence to monitor the security controls in the information system on an ongoing basis. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes establishment of defined frequencies of no less than once every 72 hours for monitoring and for assessments supporting such monitoring, and ongoing security control assessments in accordance with the organizational continuous monitoring strategy.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization uses automated tools to identify FTI on system components to ensure controls are in place to protect organizational information and individual privacy.
Level HIX Implementation Requirements	
Level PCI Implementation Requirements	
Level PCI Implementation (example):	When being assessed as a service provider, the organization performs reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: daily log reviews; firewall rule-set reviews; applying configuration standards to new systems; responding to security alerts; and change management processes. When being assessed as a service provider, the organization maintains documentation of quarterly review process to include: documenting results of the reviews, and review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization uses automated tools to identify information by information type on system components to ensure controls are in place to protect organizational information and individual privacy. The organization develops a system-wide continuous monitoring strategy and implement continuous monitoring programs that includes establishing defined frequencies, but no less than once every 72 hours for monitoring and assessment of control effectiveness.

Control Reference: 06.h Technical Compliance Checking

Control Specification:	Information systems shall be regularly checked for compliance with security implementation standards.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization performs annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools. If any non-compliance is found as a result of a technical security configuration compliance review, the organization: determines the causes of the non-compliance; evaluates the need for actions to ensure that non-compliance do not recur; determines and implements appropriate corrective action; and reviews the corrective action taken.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) CIS Controls v7.1 - CIS CSC v7.1 11.1 CIS Controls v7.1 - CIS CSC v7.1 11.3 COBIT 5 DS5.5 COBIT 5 DSS05.07 ISO/IEC 27799:2016 18.2.2 ISO/IEC 27799:2016 18.2.3 NIST Cybersecurity Framework v1.1 - DE.CM-8 NIST Cybersecurity Framework v1.1 - DE.DP-3 NIST Cybersecurity Framework v1.1 - ID.RA-1 NIST Cybersecurity Framework v1.1 - RS.MI-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High)

Level 2 Implementation (example):	Technical compliance checking is performed by an experienced technical specialist, with the assistance of industry standard automated tools, with tools which generate a technical report for subsequent interpretation, at least annually, and more frequently where needed based on risk as part of an official risk assessment process. Technical compliance checking has been implemented to show compliance in support of technical interoperability.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC4.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05 (HIGH; MOD) COBIT 5 DS5.5 HIPAA Security Rule - § 164.308(a)(8) ISO/IEC 27799:2016 18.2.3 NIST Cybersecurity Framework v1.1 - DE.CM-8
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization uses file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The file integrity checking tools reporting system: has the ability to account for routine and expected changes; highlights and alerts on unusual or unexpected changes; shows the history of configuration changes over time; and identifies who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks also identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes). The organization uses an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information, blocks such transfers, and alerts information security professionals.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization includes, as part of security control assessments, within every 365 days: announced or unannounced, in-depth system monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and penetration performance/load testing.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization includes as part of its security control assessments, within every 365 days, announced vulnerability scanning.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization performs security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system performs security compliance checks, as defined by the RMH, on constituent system components prior to the establishment of the internal connection.

	The organization requires all applications and systems to undergo periodic security compliance assessments to ensure that they reflect a security posture commensurate with each State Entity's (SEs) definition of acceptable risk. Security compliance assessments include assessments for compliance with all federal, state, and external compliance standards for which the SE is required to comply.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	The organization has implemented tools and technologies that meet stakeholder needs to operationalize Data Governance.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The organization configures the information system to provide only essential capabilities, prohibits or restricts the use of functions, ports, protocols, and/or services in accordance with Center for Internet Security guidelines (Level 1) to establish configuration settings, and ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible.

Objective Name: 06.03 Information System Audit Considerations

Control Objective:	Ensure the integrity and effectiveness of the information systems audit process.
Control Reference: 06.i Information Systems Audit Controls	
Control Specification:	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to, to minimize the risk of disruptions to business processes.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization determines which of the following auditable events require auditing on a continuous basis in response to specific situations: user log-on and log-off (successful or unsuccessful); configuration changes; application alerts and error messages; all system administration activities; modification of privileges and access; account creation, modification, or deletion; concurrent log on from different workstations; and override of access control mechanisms.

Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.02(b)(3) 23 NYCRR 500 - 500.06(a)(2) 23 NYCRR 500 - 500.14(a) HIPAA Security Rule - § 164.308(a)(1)(ii)(D) IRS Pub 1075 - AC-2g ISO/IEC 27002:2022 - 8(15) MARS-E v2.2 - AU-2d1i MARS-E v2.2 - AU-2d1ii MARS-E v2.2 - AU-2d1iii MARS-E v2.2 - AU-2d1iv MARS-E v2.2 - AU-2d1v MARS-E v2.2 - AU-2d1vi MARS-E v2.2 - AU-2d1vii NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2g NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2a] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2b] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2c] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2d] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2e] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2f] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2g] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.2h] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2c
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The organization formally addresses in audit policies and/or standards: purpose of audit and accountability requirements/controls; scope of audit and accountability requirements/controls; roles; responsibilities; management commitment of audit and accountability; coordination among organizational entities for audit and accountability; and compliance with audit and accountability requirements. The organization facilitates the implementation of audit and accountability requirements/controls.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC5.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-02 (HIGH; MOD) HIPAA Security Rule - § 164.312(b) ISO/IEC 27001:2022 - 9.2.1a1 NIST Cybersecurity Framework v1.1 - DE.DP-1

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization determines, based on a risk assessment and mission/business needs, that the information system is capable of auditing the following events: System access, including unsuccessful and successful login attempts, to information systems containing personally identifiable information (PII); Successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository; Privileged activities or system level access to PII; Concurrent logons from different workstations; and All program initiations (e.g., executable file).

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization configures information systems to audit the following events, including the frequency of (or situation requiring) auditing for each identified event: successful and unsuccessful account logon events; account management events; object access; policy change; privilege functions; process tracking; and system events. The organization determines that web applications are configured to audit the following events, including the frequency of (or situation requiring) auditing for each identified event: all administrator activity; authentication checks; authorization checks; data deletions; data access; data changes; and permission changes.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization determines, based on a risk assessment and CMS mission/business needs, that the information system can audit the following events: Server alerts and error messages; User log-on and log-off (successful or unsuccessful); All system administration activities; Modification of privileges and access; Start up and shut down; Application modifications; Application alerts and error messages; Configuration changes; Account creation, modification, or deletion; File creation and deletion; Read access to sensitive information; Modification to sensitive information; Printing sensitive information; Anomalous (e.g., non-attributable) activity; Data as required for privacy monitoring privacy controls; Concurrent log on from different work stations; Override of access control mechanisms; and Process creation. The organization determines that privileged activities or system level access to PII is audited within the information system.

Control Reference: 06.j Protection of Information Systems Audit Tools

Control Specification:	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records

Level 1 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 1 Regulatory Factors:	FedRAMP Banking Requirements PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	Access to information systems audit tools is protected to prevent any possible misuse or compromise.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-09 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 FedRAMP - AU-9[H] FedRAMP - AU-9[L] FedRAMP - AU-9[M] IRS Pub 1075 - AU-9a ISO/IEC 27799:2016 6.1.2 MARS-E v2.2 - AU-9 NIST Cybersecurity Framework v1.1 - DE.DP-1 NY OHIP Moderate-Plus Security Baseline v5.0 - AU-9a PCI DSS v3.2.1 6.4.2 Supplemental Requirements - SR v6.4 31-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Access to system audit tools is documented, enforced per a formal procedure, restricted to authorized individuals only, and approved by designated system owners. Use of these system audit tools are only authorized after receiving permission from system owners and as part of a documented assessment process. Specific controls identified within the access control policy are enforced for the audit tools. Audits of these controls are performed at least annually.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) FedRAMP - AU-6(7)[H] FedRAMP - AU-9(4)[H] FedRAMP - AU-9(4)[M] IRS Pub 1075 - AU-6(7) IRS Pub 1075 - AU-9(4) ISO/IEC 27799:2016 12.7.1 NIST Cybersecurity Framework v1.1 - DE.DP-1 NIST Cybersecurity Framework v1.1 - DE.DP-3 NIST SP 800-171 r2 - 3.3.9[a] NIST SP 800-171 r2 - 3.3.9[b] NIST SP 800-53 R4 AU-9(5)[S]{2} NIST SP 800-53 r5 - AU-9(5)
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and is defined in the applicable system security plan.

Control Category: 07.0 - Asset Management

Objective Name: 07.01 Responsibility for Assets

Control Objective:	To ensure that management requires ownership and defined responsibilities for the protection of information assets.
Control Reference: 07.a Inventory of Assets	
Control Specification:	All assets including information shall be clearly identified and an inventory of all assets drawn up and maintained.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 1 System Factors:	

Level 1 Regulatory Factors:	DirectTrust FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CA Civil Code § 1798.81.5 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 1 Implementation (example):	The organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites). The organization documents the importance of these inventoried assets. The asset inventory includes: all systems connected to the network; the network devices themselves; desktops; servers; network equipment (routers, switches, firewalls, etc.); printers; storage area networks; Voice Over-IP telephones; multi-homed addresses; virtual addresses; mobile phones, regardless of whether they are attached to the organization's network; tablets, regardless of whether they are attached to the organization's network; laptops, regardless of whether they are attached to the organization's network; other portable electronic devices [i.e., other than mobile phones, tablets, and laptops] that store or process data, regardless of whether they are attached to the organization's network; and approved bring your own device (BYOD) equipment. The asset inventories include: type or classification of the asset; format of the asset; location of the asset; backup information of the asset; license information of the asset; a business value of the asset; and data on whether the device is a portable and/or personal device. The asset inventory record is used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department. The asset inventory records: the network addresses; the machine name(s); the purpose of each system; an asset owner responsible for each device; and the department associated with each device. The inventory does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned. Records of property assigned to employees is reviewed and updated annually.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(c) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.16(a) Banking Requirements - FFIEC IS v2016 A.6.6 CIS Controls v7.1 - CIS CSC v7.1 1.4 CIS Controls v7.1 - CIS CSC v7.1 1.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-05 (HIGH; MOD) COBIT 5 APO12.03 FedRAMP - CM-8(1)[H] FedRAMP - CM-8(1)[M] Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 5.M.A Health Industry Cybersecurity Practices - 5.M.B Health Industry Cybersecurity Practices - 5.M.C Health Industry Cybersecurity Practices - 5.M.D Health Industry Cybersecurity Practices - 5.S.A Health Industry Cybersecurity Practices - 5.S.B Health Industry Cybersecurity Practices - 5.S.C Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.D HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(iii) HITRUST De-ID Framework - De-ID Framework v1 Data Storage: General IRS Pub 1075 - 3.3.5(3) IRS Pub 1075 - 3.3.6(6) IRS Pub 1075 - CM-8(1) ISO/IEC 27799:2016 8.1.1 MARS-E v2.2 - CM-8(1) MARS-E v2.2 - PM-5 NIST Cybersecurity Framework v1.1 - ID.AM-1 NIST Cybersecurity Framework v1.1 - ID.AM-2 NIST SP 800-171 r2 - 3.4.1[f] NIST SP 800-53 R4 CM-8(1)[HM]{0} NIST SP 800-53 R4 CM-8(7)[S]{0} NIST SP 800-53 R4 CM-8a[HML]{1} NIST SP 800-53 R4 CM-8b[HML]{1} NIST SP 800-53 R4 PE-20a[S]{0} NIST SP 800-53 R4 PM-5[HML]{2} NIST SP 800-53 r5 - CM-8(1) NIST SP 800-53 r5 - CM-8(7) NIST SP 800-53 r5 - CM-8a NIST SP 800-53 r5 - CM-8b NIST SP 800-53 r5 - PE-20 NIST SP 800-53 r5 - PM-5 NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8[IS.2] PCI DSS v3.2.1 12.3.3 Veterans Affairs Cybersecurity Program Directive 6500 - a(1)(c) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(j)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Are wireless access points in place at any of the organization's in-scope facilities? No
Level 2 Regulatory Factors:	Community Supplemental Requirements 002 DirectTrust HITRUST De-ID Framework PCI DSS v3.2.1 Texas Medical Records Privacy Act High Low Moderate Supplemental
Level 2 Implementation (example):	The information lifecycle manages the secure use, transfer, exchange, and disposal of IT-related assets. The organization maintains an inventory of authorized wireless access points (WAPs). The inventory of WAPs includes a documented business justification and supports unauthorized WAP identification and response.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 AICPA Trust Services Criteria - AICPA 2017 CC6.5 Banking Requirements - FFIEC IS v2016 A.6.16(e) Banking Requirements - FFIEC IS v2016 A.6.6 CIS Controls v7.1 - CIS CSC v7.1 15.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-01 (HIGH; MOD) Community Supplemental Requirements 002 - CSR002 v2018 11.2-4-2 HIPAA Security Rule - § 164.308(a)(7)(ii)(E) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(i) HIPAA Security Rule - § 164.310(d)(2)(ii) HIPAA Security Rule - § 164.310(d)(2)(iii) HITRUST ISO/IEC 27002:2022 - 7(10) ISO/IEC 27799:2016 8.1.1 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.DS-3 NIST Cybersecurity Framework v1.1 - RS.AN-2 NIST SP 800-171 r2 - 3.1.16[a] NIST SP 800-53 R4 CM-8a[HML]{2} NIST SP 800-53 R4 SA-19(3)[S]{0} NIST SP 800-53 R4 SI-13(3)[S]{0} NIST SP 800-53 r5 - AC-4(25) NIST SP 800-53 r5 - CM-8a NIST SP 800-53 r5 - RA-9 NIST SP 800-53 r5 - SA-3(3) NIST SP 800-53 r5 - SI-13(3) NIST SP 800-53 r5 - SR-12 PCI DSS v3.2.1 11.1.1 PCI DSS v3.2.1 12.3.3 PCI DSS v3.2.1 2.4 PCI DSS v3.2.1 9.7.1 PCI DSS v3.2.1 9.9 PCI DSS v3.2.1 9.9.1 Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(a)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	

Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 3 Implementation (example):	The IT asset lifecycle program is monitored to ensure it effectively addresses all six stages of the lifecycle: planning - defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts; procurement - requisitioning, approving requisitions, ordering, receiving, and validating orders; deployment - tagging assets, entering asset information in a repository, configuring and installing assets including: disabling unnecessary or insecure services or protocols, limiting servers to one primary function, and defining system security parameters to prevent misuse; management - inventory/counting, monitoring usage (some software), managing contracts for maintenance and support, and monitoring age and configuration; support - adding and changing configurations, repairing devices, and relocating equipment and software; and disposition - removing assets from service, deleting storage contents, disassembling components for reuse, surplussing equipment, terminating contracts, disposing of equipment, and removing assets from active inventory. The organization: employs automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized components/devices (including hardware, firmware, and software) into the information system; disables network access by such components/devices; and notifies designated organizational officials of such unauthorized components/devices.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC7.1 Banking Requirements - FFIEC IS v2016 A.6.16(b) Banking Requirements - FFIEC IS v2016 A.6.16(c) Banking Requirements - FFIEC IS v2016 A.6.16(d) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SE-01 (HIGH; MOD) FedRAMP - SI-4(22)[H] Health Industry Cybersecurity Practices - 5.S.B HIPAA Security Rule - § 164.310(d)(2)(iii) IRS Pub 1075 - CM-7(9)a MARS-E v2.2 - CM-8(3)a MARS-E v2.2 - CM-8a1 MARS-E v2.2 - RA-2d NIST Cybersecurity Framework v1.1 - PR.DS-8 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST Cybersecurity Framework v1.1 - RS.AN-5 NIST SP 800-53 R4 CM-11(1)[S]{0} NIST SP 800-53 R4 CM-8(3)[HM]{0} NIST SP 800-53 R4 SA-10(6)[S]{2} NIST SP 800-53 R4 SA-19(4)[S]{0} NIST SP 800-53 R4 SA-19[S]{0} NIST SP 800-53 R4 SC-7(14)[S]{0} NIST SP 800-53 R4 SI-13(1)[S]{0} NIST SP 800-53 R4 SI-4(22)[S]{0} NIST SP 800-53 r5 - CM-8(3) NIST SP 800-53 r5 - SA-10(6) NIST SP 800-53 r5 - SC-7(14) NIST SP 800-53 r5 - SI-13(1) NIST SP 800-53 r5 - SI-4(22) NIST SP 800-53 r5 - SR-11(3) NIST SP 800-53 r5 - SR-4(3) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8(3)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8(3)a Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(m) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(n)

Level CIS Implementation Requirements

Level CIS Implementation (example):	The organization uses a software inventory tool to automate the documentation of all software on business systems. The software inventory tool tracks the name, version, publisher, and install date of all software, including operating systems, unauthorized by the organization. The organization has deployed an active and passive automated asset discovery tool(s) and uses it to build/maintain/reconcile an asset inventory of systems connected to its public and private network(s).

Level CMS Implementation Requirements

Level CMS Implementation (example):	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories. In addition to the creation of the IT asset lifecycle program, the organization identifies an owner to manage all organization IT asset inventory and management-related process and procedure documents.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization reviews and updates the information system component inventory at least monthly.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization maintains an inventory which accounts for master keys and key duplicates, and performs an annual reconciliation on all key records. The organization reviews and updates the list of authorized hardware components annually.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization maintains an inventory of system components that are in scope for PCI DSS. The inventory of system components and devices in scope for PCI DSS identify all personnel authorized to use the system components and devices. Lists of payment card devices are kept up-to-date, and include the following: make, model of device; location of device (for example, the address of the site or facility where the device is located); and device serial number or other method of unique identification.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization's asset inventory does not duplicate other inventories unnecessarily, but will ensure that the content is aligned. The organization develops and documents an inventory of information system components that includes: Each component's unique identifier and/or serial number; Information system of which the component is a part; Type of information system component (e.g., server, desktop, application); Manufacturer/model information; Operating system type and version/service pack level; Presence of virtual machines; Application software version/license information; Physical location (e.g., building/room number); Logical location (e.g., IP address, position with the information system [IS] architecture); Media access control (MAC) address; Ownership; Operational status; Primary and secondary administrators; and Primary user.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization: establishes, maintains, and updates within organization-defined frequency an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and provides each update of the PII inventory to the CIO or information security official within organization-defined frequency to support the establishment of information security requirements for all new or modified information systems containing PII.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	Upon the successful disposal or sanitization of an IT asset, the IT asset management record of the asset is updated to reflect that it has been decommissioned and is no longer owned by the organization.
Level ISO/IEC 23894 Implementation Requirements	
Level ISO/IEC 23894 Implementation (example):	The organization maintains an inventory of AI data, models, and systems that it uses and/or develops.

Control Reference: 07.b Ownership of Assets

Control Specification:	All information and assets associated with information processing systems shall be owned by a designated part of the organization.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	PCI DSS v3.2.1 High Low Moderate Supplemental
Level 1 Implementation (example):	All information systems are documented. Documentation of all information systems includes a method to determine accurately and readily the: assigned owner of responsibility; owner's contact information; and purpose (e.g., through labeling, coding, and/or inventory).
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08 (HIGH; MOD) Health Industry Cybersecurity Practices - 5.M.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.310(d)(2)(iii) NIST SP 800-53 R4 CM-8(9)a[S]{0} NIST SP 800-53 R4 PM-5[HML]{1} NIST SP 800-53 r5 - CM-8(9)a NIST SP 800-53 r5 - PM-5 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-5 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-5[IS.1] PCI DSS v3.2.1 12.3.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The asset owner is responsible for: ensuring that information and assets associated with information processing systems are appropriately classified; and defining and periodically (at a minimum, annually) reviewing access restrictions and classifications, taking into account applicable access control policies. The organization allocates asset responsibility based on a business process, a defined set of activities, an application, or a defined set of data. All information and assets associated with information processing systems are assigned responsibility to a designated part of the organization. All information has an information owner or owners (e.g., designated individuals responsible) established within the organization's lines of business.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.6 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-10 (HIGH; MOD) ISO/IEC 27001:2022 - 6.1.2c2 ISO/IEC 27002:2022 - 5(9) ISO/IEC 27799:2016 8.1.2 NIST SP 800-53 R4 CM-10a[HML]{0} NIST SP 800-53 R4 CM-8(9)b[S]{0} NIST SP 800-53 R4 PS-3(2)[S]{2} NIST SP 800-53 r5 - AC-16(1) NIST SP 800-53 r5 - AC-16(10) NIST SP 800-53 r5 - AC-16(3) NIST SP 800-53 r5 - AC-16(4) NIST SP 800-53 r5 - AC-16(6) NIST SP 800-53 r5 - AC-16(7) NIST SP 800-53 r5 - CM-10a NIST SP 800-53 r5 - CM-8(9)b NY OHIP Moderate-Plus Security Baseline v5.0 - CP-1[PRIV.1] Veterans Affairs Cybersecurity Program Directive 6500 - a(1)(a) Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(a) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(h)
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization reviews accounts for compliance with account management requirements monthly for privileged access and every six months for non-privileged access.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	All FTI has a management official, e.g., an accrediting authority, assigned as an owner to provide responsibility and accountability for its protection.
Level VA Directive 6500 Implementation Requirements	
Level VA Directive 6500 Implementation (example):	The organization registers all Veterans Affairs (VA) Information Systems in the VA System Inventory (VASI) in accordance with VA policy and as part of a security authorization in VA's Governance, Risk and Compliance tool at the Department level.

Control Reference: 07.c Acceptable Use of Assets	
Control Specification:	Rules for the acceptable use of information and assets associated with information processing systems shall be identified, documented, and implemented.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA The Joint Commission v2016 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization establishes and makes readily available to all information system users a set of rules that describe their responsibilities and expected behavior with regard to information and information system usage. Acceptable use addresses rules for electronic mail and Internet usages and guidelines for the use of mobile devices, especially for the use outside the premises of the organization. The organization includes in the rules of behavior containing explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.18(g) Banking Requirements - FFIEC IS v2016 A.6.8(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04(01) (HIGH; MOD) FedRAMP - PL-4(1)[H] FedRAMP - PL-4(1)[M] FedRAMP - PL-4a[H] FedRAMP - PL-4a[L] FedRAMP - PL-4a[M] Health Industry Cybersecurity Practices - 4.S.C HIPAA Security Rule - § 164.310(b) IRS Pub 1075 - 3.3.2(1)a IRS Pub 1075 - PL-4(1)a IRS Pub 1075 - PL-4(1)b IRS Pub 1075 - PL-4(1)c IRS Pub 1075 - PL-4a ISO/IEC 27799:2016 8.1.3 MARS-E v2.2 - PL-4(1) MARS-E v2.2 - PL-4a1 MARS-E v2.2 - PL-4a2 NIST SP 800-53 R4 PL-4(1)[HM]{0} NIST SP 800-53 R4 PL-4a[HML]{0} NIST SP 800-53 r5 - PL-4(1)a NIST SP 800-53 r5 - PL-4(1)b NIST SP 800-53 r5 - PL-4(1)c NIST SP 800-53 r5 - PL-4a NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4(1)b NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4(1)c NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4a1 NY OHIP Moderate-Plus Security Baseline v5.0 - PL-4a2 PCI DSS v3.2.1 12.3 PCI DSS v3.2.1 12.3.5 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(c) The Joint Commission (v2016) - TJC IM.02.01.03, EP 1 Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(a)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA The Joint Commission v2016 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The organization confirms employees, contractors, and third-party users using or having access to the organization’s assets are made aware of the limits existing for their use of the organization’s information and assets associated with information processing facilities, and resources. Users are responsible for their use of any information processing resources, and of any such use carried out under their responsibility.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.18(g) Banking Requirements - FFIEC IS v2016 A.6.8(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) ISO/IEC 27799:2016 8.1.3 MARS-E v2.2 - PL-4e The Joint Commission (v2016) - TJC IM.02.01.03, EP 1

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The organization reviews and updates the rules of behavior annually, receives signed acknowledgments from users indicating that they have read, understand, and agree to abide by the rules of behavior before access to information and the information system is authorized, and requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Objective Name: 07.02 Information Classification

Control Objective:	To ensure that information receives an appropriate and consistent level of protection.

Control Reference: 07.d Classification Guidelines

Control Specification:	Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	Banking Requirements Supplemental

Level 1 Implementation (example):	The organization establishes a classification schema to differentiate between various levels of sensitivity and value. Information assets are classified according to their level of sensitivity as follows: Level 1: Low-sensitive information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal, or hard copy; Level 2: Sensitive information that may not to be protected from public disclosure but if made easily and readily available, the organization will follow its disclosure policies and procedures before providing this information to external parties; Level 3: Sensitive information intended for limited business use that can be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of employees, clients, or partners; Level 4: Information that is deemed extremely sensitive and is intended for use by named individuals only. This information is typically exempt from public disclosure. Users of information systems will be notified and made aware when the data they are accessing contains PII.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.03(b) Banking Requirements - FFIEC IS v2016 A.6.6 Health Industry Cybersecurity Practices - 10.M.A Health Industry Cybersecurity Practices - 4.M.A Health Industry Cybersecurity Practices - 4.M.B Health Industry Cybersecurity Practices - 4.S.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HITRUST ISO/IEC 27002:2022 - 5(12) ISO/IEC 27799:2016 8.2.1 NIST Cybersecurity Framework v1.1 - ID.AM-5 NIST SP 800-53 R4 AC-16d[S]{0} NIST SP 800-53 r5 - AC-16d

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Community Supplemental Requirements 002 FedRAMP FISMA The Joint Commission v2016 CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	The organization processing PII uniformly classifies such data as sensitive, confidential, or similar, which means that there are limitations to its disclosure within the organization and externally. The organization categorizes (classifies) records by type (e.g., accounting records, database records, transaction logs, audit logs and operational procedures) with details of storage media and document the results. Classifications and associated protective controls for information take account of: business needs for sharing or restricting information; the business impacts associated with such needs; and the aggregation effect.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.6 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-02 (HIGH; MOD) Community Supplemental Requirements 002 - CSR002 v2018 11.2-4-1 FedRAMP - RA-2b[H] FedRAMP - RA-2b[L] FedRAMP - RA-2b[M] Health Industry Cybersecurity Practices - 10.S.A Health Industry Cybersecurity Practices - 4.L.B HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(8) HIPAA Security Rule - § 164.310(d)(2)(iii) HIPAA Security Rule - § 164.312(c)(1) HITRUST ISO/IEC 27002:2022 - 5(12) ISO/IEC 27799:2016 ISO/IEC 27799:2016 8.1.1 ISO/IEC 27799:2016 8.1.2 ISO/IEC 27799:2016 8.2.1 MARS-E v2.2 - RA-2b NIST Cybersecurity Framework v1.1 - ID.RA-4 NIST Cybersecurity Framework v1.1 - ID.RA-5 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST Cybersecurity Framework v1.1 - PR.PT-2 NIST Cybersecurity Framework v1.1 - RS.AN-4 NIST SP 800-53 R4 AC-16(1)[S]{0} NIST SP 800-53 R4 AC-16(10)[S]{1} NIST SP 800-53 R4 AC-16(10)[S]{2} NIST SP 800-53 R4 AC-16(2)[S]{1} NIST SP 800-53 R4 AC-16(3)[S]{0} NIST SP 800-53 R4 AC-16(4)[S]{0} NIST SP 800-53 R4 AC-16(6)[S]{0} NIST SP 800-53 R4 AC-16(7)[S]{2} NIST SP 800-53 R4 AC-16(8)[S]{2} NIST SP 800-53 R4 AC-16(9)[S]{0} NIST SP 800-53 R4 PL-8a[HM]{2} NIST SP 800-53 R4 PM-11b[HML]{0} NIST SP 800-53 R4 RA-2a[HML]{0} NIST SP 800-53 R4 RA-2b[HML]{0} NIST SP 800-53 r5 - AC-16(1) NIST SP 800-53 r5 - AC-16(2) NIST SP 800-53 r5 - AC-16(6) NIST SP 800-53 r5 - AC-16(8) NIST SP 800-53 r5 - AC-16(9) NIST SP 800-53 r5 - AC-16f NIST SP 800-53 r5 - AC-3(11) NIST SP 800-53 r5 - AC-3(13) NIST SP 800-53 r5 - PT-2(1) NIST SP 800-53 r5 - RA-2a NIST SP 800-53 r5 - RA-2b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-8[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-2[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-2[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-2[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-2b The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Level 2 Authoritative Source Mapping (Cont.):	Veterans Affairs Cybersecurity Program Directive 6500 - a(1)(c)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Authoritative Source Mapping:	
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative.
Level FTI Custodians Implementation Requirements	
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization employs data tags to automate the correction and deletion of personally identifiable information (PII) across the information life cycle within organizational systems.
Control Reference: 07.e Information Labeling and Handling	
Control Specification:	An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act Supplemental
Level 1 Implementation (example):	The organization physically and/or electronically labels and handles sensitive information commensurate with the risk of the information or document. Labeling reflects the classification according to the rules in the information classification policy.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(ii) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(vi) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(vii) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(B)(iv) AICPA Trust Services Criteria - AICPA 2017 C1.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-03 (HIGH; MOD) Health Industry Cybersecurity Practices - 4.M.B Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HITRUST ISO/IEC 27002:2022 - 5(13) NIST SP 800-171 r2 - 3.8.4[a] NIST SP 800-171 r2 - 3.8.4[b] NIST SP 800-53 R4 AC-16(5)[S]{1} NIST SP 800-53 R4 AC-4(18)[S]{0} NIST SP 800-53 r5 - AC-16(5) NIST SP 800-53 r5 - PT-3(1) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(g)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Items requiring labeling include printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, electronic messages, and file transfers). The organization may exempt specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.04(b)(1) AICPA Trust Services Criteria - AICPA 2017 C1.2 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-03 (HIGH; MOD) Health Industry Cybersecurity Practices - 4.M.B ISO/IEC 27002:2022 - 5(13) ISO/IEC 27799:2016 16.1.7 ISO/IEC 27799:2016 8.2.2 ISO/IEC 27799:2016 8.2.3 MARS-E v2.2 - MP-3b NIST Cybersecurity Framework v1.1 - PR.DS-1 NIST Cybersecurity Framework v1.1 - PR.DS-2 NIST Cybersecurity Framework v1.1 - PR.IP-6 NIST SP 800-53 R4 AC-16(7)[S]{1} NIST SP 800-53 R4 AC-16a[S]{0} NIST SP 800-53 R4 AC-16c[S]{0} NIST SP 800-53 R4 PE-5(3)[S]{0} NIST SP 800-53 r5 - AC-16(7) NIST SP 800-53 r5 - AC-16a NIST SP 800-53 r5 - AC-16c NIST SP 800-53 r5 - CM-12(1) NIST SP 800-53 r5 - MP-3 NIST SP 800-53 r5 - PL-2a5 NIST SP 800-53 r5 - PT-3(1) NY OHIP Moderate-Plus Security Baseline v5.0 - MP-3[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-3b PCI DSS v3.2.1 9.6.1
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP
Level 3 Implementation (example):	Information belonging to different classification levels are logically or physically separated. Whenever possible information assets classified as critical are stored in a separate, secure area. All information systems processing covered information (e.g., PII) inform users of the confidentiality of covered information accessible from the system (e.g., at start-up or log-in).
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-08 (HIGH; MOD) NIST SP 800-171 r2 - 3.1.9[a] NIST SP 800-171 r2 - 3.1.9[b]

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization labels removable media and information system output containing FTI to indicate the distribution limitations and handling caveats (note IRS Notice 129-A or Notice 129-B are available for this purpose). The organization properly labels emails that contain FTI (e.g., email subject contains FTI) to ensure that the recipient is aware that the message content contains FTI.
Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation (example):	Patient information subject to special handling, e.g., HIV test results and mental health and substance abuse-related records, is identified and appropriately labeled. Handling requirements for patient information subject to special handling, e.g., HIV test results and mental health and substance abuse-related records, are: expressly defined consistent with applicable federal and state legislative and regulatory requirements and industry guidelines; and implemented consistent with applicable federal and state legislative and regulatory requirements and industry guidelines. The freestanding emergency medical facilities: require implementation of the Health and Human Services Executive Commissioner's minimum standards for the contents of medical records; require implementation of the Health and Human Services Executive Commissioner's minimum standards for the maintenance of medical records; require implementation of the Health and Human Services Executive Commissioner's minimum standards for the release of medical records; have designated an individual to be in charge of the creation, maintenance, and disposal of medical records per 25 TAC § 131.53; and have standards including the confidentiality, security, and safe storage of medical records throughout the records lifecycle.
Level HIPAA Implementation Requirements	
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	If Personally Identifiable Information (PII) or Protected Health Information (PHI) is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions. Stored data must have at a minimum, the following data, clearly identifiable by labels or other approved coding systems: The System Name, Creation Date, Sensitivity Classification (based on applicable record retention regulations), CMS Contact Information.

Control Category: 08.0 - Physical and Environmental Security

Objective Name: 08.01 Secure Areas

Control Objective:	To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Control Reference: 08.a Physical Security Perimeter	
Control Specification:	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information assets.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust Texas Medical Records Privacy Act
Level 1 Implementation (example):	Computers that store or process covered and/or confidential information are located in rooms with doors and windows that are locked when unattended, and are not located in areas that are unattended and have unrestricted access by the public. External protection is considered for windows, particularly at ground level (public, sensitive, and restricted areas).
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) Banking Requirements - FFIEC IS v2016 A.6.21(c) Banking Requirements - FFIEC IS v2016 A.6.8 Health Industry Cybersecurity Practices - 6.S.B HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - 2.B.3.3(6) ISO/IEC 27799:2016 11.1.1 ISO/IEC 27799:2016 11.2.6
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust HITRUST De-ID Framework PCI DSS v3.2.1 Texas Medical Records Privacy Act High Low Moderate

Level 2 Implementation (example):	Perimeters of a building or site containing information assets are physically sound; there are no gaps in the perimeter or areas where a break-in could easily occur. The external walls of the site are of solid construction. All external doors are protected against unauthorized access with control mechanisms (e.g., bars, alarms, locks etc.). Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks) are documented and retained in accordance with the organization's retention policy.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.4 Banking Requirements - FFIEC IS v2016 A.6.8 Banking Requirements - FFIEC IS v2016 A.8.1(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-24 (HIGH; MOD) COBIT 5 DSS05.05 HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.310(a)(2)(iv) HIPAA Security Rule - § 164.310(c) HITRUST De-ID Framework - De-ID Framework v1 Public Access to Sensitive Areas: General IRS Pub 1075 - 2.B.3(3) IRS Pub 1075 - 2.B.3.4(8) IRS Pub 1075 - 3.3.6(1) ISO/IEC 27002:2022 - 7(1) ISO/IEC 27002:2022 - 7(2) ISO/IEC 27002:2022 - 7(3) ISO/IEC 27002:2022 - 8(32) ISO/IEC 27799:2016 11.1.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - MA-2a MARS-E v2.2 - PE-3a1 NIST Cybersecurity Framework v1.1 - DE.CM-2 NIST Cybersecurity Framework v1.1 - DE.DP-2 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 R4 PE-3e[HML]{2} NIST SP 800-53 r5 - PE-3(7) NIST SP 800-53 r5 - PE-3(8) NIST SP 800-53 r5 - PE-3e NY OHIP Moderate-Plus Security Baseline v5.0 - PE-3[IS.3] OCR Audit Protocol (2016) 164.310(a)(2)(iv) PCI DSS v3.2.1 9.1
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	

Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements CMS Minimum Security Requirements (High)
Level 3 Implementation (example):	The organization ensures information assets and facilities it manages are physically separated from those managed by third-parties. Two barriers to access covered information under normal security are required: secured perimeter/locked container; locked perimeter/secured interior; or locked perimeter/security container.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-03 (HIGH; MOD) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - 2.B.2(1) IRS Pub 1075 - 2.B.2(2) ISO/IEC 27799:2016 11.1.1 MARS-E v2.2 - PE-3a1
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Two physical barriers between FTI and an individual not authorized to access FTI are used, including a combination of a secured perimeter, a security room, badged employees, and a security container. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access afterhours. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably work above the waist. The perimeter is enclosed by slab-to-slab walls constructed of durable materials. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. The perimeter walls are periodically inspected.

Control Reference: 08.b Physical Entry Controls

Control Specification:	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate

Level 1 Implementation (example):	Access to areas where sensitive information (e.g., covered information, payment card data) is processed or stored is controlled and restricted to authorized persons only. For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points to the facility, maintains physical access audit logs, and provides security safeguards the organization determines are necessary for areas officially designated as publicly accessible.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) Banking Requirements - FFIEC IS v2016 A.6.8 Banking Requirements - FFIEC IS v2016 A.8.1(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-03 (HIGH; MOD) COBIT 5 DSS05.05 FedRAMP - PE-3a1[H] FedRAMP - PE-3a1[L] FedRAMP - PE-3a1[M] FedRAMP - PE-3b[H] FedRAMP - PE-3b[L] FedRAMP - PE-3b[M] FedRAMP - PE-3c[H] FedRAMP - PE-3c[L] FedRAMP - PE-3c[M] Health Industry Cybersecurity Practices - 6.M.E Health Industry Cybersecurity Practices - 6.S.B Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Privacy Rule - 164.504(e)(2)(ii)(B) HIPAA Security Rule - § 164.308(a)(3)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.310(c) HIPAA Security Rule - § 164.312(a)(1) IRS Pub 1075 - 2.B.3.4(5) IRS Pub 1075 - PE-3a1 IRS Pub 1075 - PE-3b IRS Pub 1075 - PE-3c ISO/IEC 27002:2022 - 7(3) ISO/IEC 27002:2022 - 8(3) ISO/IEC 27799:2016 11.1.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PE-3b MARS-E v2.2 - PE-3c NIST SP 800-171 r2 - 3.10.2[a] NIST SP 800-171 r2 - 3.10.2[b] NIST SP 800-171 r2 - 3.10.2[c] NIST SP 800-171 r2 - 3.10.2[d] NIST SP 800-53 R4 PE-3a[HML]{1} NIST SP 800-53 R4 PE-3b[HML]{0} NIST SP 800-53 R4 PE-3c[HML]{0} NIST SP 800-53 r5 - PE-3a NIST SP 800-53 r5 - PE-3b NIST SP 800-53 r5 - PE-3c NY OHIP Moderate-Plus Security Baseline v5.0 - PE-3b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-3c PCI DSS v3.2.1 9.4 Supplemental Requirements - SR v6.4 8a-0 Supplemental Requirements - SR v6.4 8b-0 Supplemental Requirements - SR v6.4 9.2-0 Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(d)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust PCI DSS v3.2.1 Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate
Level 2 Implementation (example):	Physical access of visitors is recorded and records contain: name of the person visiting; organization of the person visiting; signature of the visitor; form of identification (shown by the visitor); date of access; time of entry; time of departure; purpose of the visit; name of person visited; and organization of person visited. All visitors are supervised unless their access has been previously approved. Third-party support personnel are granted restricted access to secure areas or to covered and/or confidential information processing facilities only when required, authorized, and monitored. The organization develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. The organization issues authorization credentials for facility access, reviews the access list and authorization credentials periodically, but no less than quarterly, and removes individuals from the facility access list when access is no longer required.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) AICPA Trust Services Criteria - AICPA 2017 CC6.1 AICPA Trust Services Criteria - AICPA 2017 CC6.2 AICPA Trust Services Criteria - AICPA 2017 CC6.3 AICPA Trust Services Criteria - AICPA 2017 CC6.4 Banking Requirements - FFIEC IS v2016 A.6.8 Banking Requirements - FFIEC IS v2016 A.8.1(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-08 (HIGH; MOD) COBIT 5 DSS05.05 FedRAMP - PE-2a[H] FedRAMP - PE-2a[L] FedRAMP - PE-2a[M] FedRAMP - PE-2b[H] FedRAMP - PE-2b[L] FedRAMP - PE-2b[M] FedRAMP - PE-2c[H] FedRAMP - PE-2c[L] FedRAMP - PE-2c[M] FedRAMP - PE-2d[H] FedRAMP - PE-2d[L] FedRAMP - PE-2d[M] FedRAMP - PE-6b[H] FedRAMP - PE-6b[L] FedRAMP - PE-6b[M] FedRAMP - PE-8a[H] FedRAMP - PE-8a[L] FedRAMP - PE-8a[M] FedRAMP - PE-8b[H] FedRAMP - PE-8b[L] FedRAMP - PE-8b[M] HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.310(c) HITRUST De-ID Framework - De-ID Framework v1 Physical Access: Identification Policy HITRUST De-ID Framework - De-ID Framework v1 Physical Access: Inappropriate Use HITRUST De-ID Framework - De-ID Framework v1 Physical Security: General HITRUST De-ID Framework - De-ID Framework v1 Visitor Access: Policy IRS Pub 1075 - PE-2a IRS Pub 1075 - PE-2b IRS Pub 1075 - PE-2c IRS Pub 1075 - PE-2d ISO/IEC 27799:2016 11.1.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PE-2a MARS-E v2.2 - PE-2b MARS-E v2.2 - PE-2c MARS-E v2.2 - PE-2d MARS-E v2.2 - PE-3a1 MARS-E v2.2 - PE-8a MARS-E v2.2 - PE-8b NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - DE.DP-2 NIST Cybersecurity Framework v1.1 - PR.AC-2

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-171 r2 - 3.10.3[a] NIST SP 800-171 r2 - 3.10.4[a] NIST SP 800-53 R4 PE-2[HML]{0} NIST SP 800-53 R4 PE-3e[HML]{1} NIST SP 800-53 R4 PE-6b[HML]{1} NIST SP 800-53 R4 PE-8[HML]{0} NIST SP 800-53 r5 - PE-2 NIST SP 800-53 r5 - PE-3e NIST SP 800-53 r5 - PE-6b NIST SP 800-53 r5 - PE-8a NIST SP 800-53 r5 - PE-8b NY OHIP Moderate-Plus Security Baseline v5.0 - MP-4[PHI.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-2a NY OHIP Moderate-Plus Security Baseline v5.0 - PE-2b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-2c NY OHIP Moderate-Plus Security Baseline v5.0 - PE-2d PCI DSS v3.2.1 9.1 PCI DSS v3.2.1 9.2 PCI DSS v3.2.1 9.3 PCI DSS v3.2.1 9.4 PCI DSS v3.2.1 9.4.1 PCI DSS v3.2.1 9.4.2 PCI DSS v3.2.1 9.4.3 PCI DSS v3.2.1 9.4.4 Supplemental Requirements - SR v6.4 9.1-0 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5 Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(d)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	Doors to internal secure areas lock automatically, implement a door delay alarm, and are equipped with electronic locks (e.g., keypad, card swipe). The organization will inventory physical access devices within every 90 days.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) Banking Requirements - FFIEC IS v2016 A.6.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-03(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-06(01) (HIGH; MOD) FedRAMP - PE-3f[H] FedRAMP - PE-3f[L] FedRAMP - PE-3f[M] FedRAMP - PE-3g[H] FedRAMP - PE-3g[L] FedRAMP - PE-3g[M] FedRAMP - PE-6(1)[H] FedRAMP - PE-6(1)[M] Health Industry Cybersecurity Practices - 5.S.B Health Industry Cybersecurity Practices - 6.S.B HIPAA Security Rule - § 164.310(d)(2)(iii) HITRUST De-ID Framework - De-ID Framework v1 Perimeter Security (Alarms): General HITRUST De-ID Framework - De-ID Framework v1 Perimeter Security (Alarms): Logging IRS Pub 1075 - 2.B.3.4(2) IRS Pub 1075 - 2.B.3.4(6)a IRS Pub 1075 - PE-3f IRS Pub 1075 - PE-3g IRS Pub 1075 - PE-6(1) ISO/IEC 27799:2016 11.1.1 MARS-E v2.2 - PE-14c MARS-E v2.2 - PE-3f MARS-E v2.2 - PE-3g MARS-E v2.2 - PE-6(1) NIST Cybersecurity Framework v1.1 - DE.DP-1 NIST SP 800-171 r2 - 3.10.5[a] NIST SP 800-171 r2 - 3.10.5[b] NIST SP 800-171 r2 - 3.10.5[c] NIST SP 800-53 R4 PE-3(3)[S]{0} NIST SP 800-53 R4 PE-3(6)[S]{0} NIST SP 800-53 R4 PE-3g[HML]{2} NIST SP 800-53 R4 PE-6(1)[HM]{0} NIST SP 800-53 R4 PE-6b[HML]{2} NIST SP 800-53 r5 - PE-3(3) NIST SP 800-53 r5 - PE-3g NIST SP 800-53 r5 - PE-6(1) NIST SP 800-53 r5 - PE-6b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-3f NY OHIP Moderate-Plus Security Baseline v5.0 - PE-3g
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.). The organization employs automated mechanisms to facilitate the maintenance and review of access records.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by controlling ingress/egress to the facility using physical access control systems/devices and guards.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	A visitor access log containing specific data elements will be used to authenticate and authorize visitors access to any facility where FTI resides, either electronically or in paper, at the location where the outside (second) barrier is breached. A restricted area visitor log will be maintained at a designated entrance to the restricted area. All visitors (persons not assigned to the area) entering the area are directed to the designated entrance. Visitor access records are corroborated against each other and include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited. The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility in areas where FTI is received, processed, stored, or transmitted.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization authorizes physical access to the facility where the information system resides and information is received, processed, stored, or transmitted, based on position or role.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization ensures visitors are authorized before entering and escorted at all times within areas where cardholder data is processed or maintained. Visitor logs include the name of the onsite personnel (workforce member) authorizing physical access.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	At a minimum, visitor access records include the following information: name of the person visiting; organization of the person visiting; visitor's signature; form of identification; date of access; time of entry; time of departure; purpose of visit; name of person visited; and organization of person visited. The organization restricts unescorted access to the facility where the information system resides to personnel with (one or more): security clearances for all information contained within the system, formal access authorizations for all information contained within the system, need for access to all information contained within the system, and/or organization-defined credentials.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization requires two forms of identification from the following forms of identification for visitor access to the facility where the system resides: passports; REAL ID-compliant drivers' licenses; Personal Identity Verification (PIV) cards; key cards; PINs; and biometrics.
Level NIST SP 800-171 Implementation Requirements	
Level NIST SP 800-171 Implementation (example):	The organization escorts visitors and monitors visitor activity.

Control Reference: 08.c Securing Offices, Rooms, and Facilities

Control Specification:	Physical security for offices, rooms, and facilities shall be designed and applied.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Relevant health and safety regulations and standards are taken into consideration when securing facilities.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) HIPAA Security Rule - § 164.308(a)(8) ISO/IEC 27799:2016 11.1.3 NIST Cybersecurity Framework v1.1 - DE.DP-2
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP HITRUST De-ID Framework Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Critical facilities are sited to avoid access by the public. For particularly sensitive and restricted facilities (e.g., data centers and communication closets) buildings are unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities. The organization ensures directories and internal telephone books identifying locations of covered information processing facilities are not readily accessible by the public.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.8 Banking Requirements - FFIEC IS v2016 A.8.1(e) CIS Controls v7.1 - CIS CSC v7.1 12.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-03 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Public Access to Sensitive Areas: General HITRUST De-ID Framework - De-ID Framework v1 Video Surveillance: General ISO/IEC 27002:2022 - 7(4) ISO/IEC 27799:2016 11.1.3 NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - RS.RP-1 NIST SP 800-53 R4 PE-6(2)[S]{0} NIST SP 800-53 R4 PE-6(3)[S]{0} NIST SP 800-53 r5 - PE-6(2) NIST SP 800-53 r5 - PE-6(3) PCI DSS v3.2.1 9.1.1

Control Reference: 08.d Protecting Against External and Environmental Threats

Control Specification:	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization develops, disseminates, and reviews/updates annually a formal, documented physical and environmental protection policy. The physical and environmental protection policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization develops formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 23 NYCRR 500 - 500.03(j) AICPA Trust Services Criteria - AICPA 2017 CC3.1 Banking Requirements - FFIEC IS v2016 A.6.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.IP-5

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Texas Medical Records Privacy Act High Moderate Supplemental
Level 2 Implementation (example):	Appropriate fire extinguishers are located throughout the facility, and are no more than fifty (50) feet away from critical electrical components. Fire detectors (e.g., smoke or heat activated) are installed on and in the ceilings and floors. Fire prevention training is included in the regular training programs provided to the organization personnel. Appropriate fire suppression systems (e.g., sprinklers, gas) are implemented throughout the building, and within secure areas containing information processing devices. For facilities not staffed continuously, these suppression systems are automated. The building's HVAC system is configured to automatically shut down upon fire detection.
Level 2 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-13 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-13(03) (HIGH; MOD) ISO/IEC 27799:2016 11.1.4 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - DE.DP-2 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 R4 AT-3(1)[S]{0} NIST SP 800-53 R4 PE-13(3)[HM]{0} NIST SP 800-53 R4 PE-13(4)[S]{0} NIST SP 800-53 r5 - AT-3(1) NIST SP 800-53 r5 - PE-13(4) NY OHIP Moderate-Plus Security Baseline v5.0 - PE-13(2)b

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements CMS Minimum Security Requirements (High) High Low Moderate
Level 3 Implementation (example):	Fire authorities are automatically notified when a fire alarm is activated. Water detectors are located in the dropped ceilings and raised floors to detect leaks or possible flooding. Master shutoff or isolation valves are accessible, working properly, and known to key personnel.
Level 3 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-13 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-13(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-13(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-15 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-15(01) (HIGH) FedRAMP - PE-13[H] FedRAMP - PE-13[L] FedRAMP - PE-13[M] FedRAMP - PE-15[H] FedRAMP - PE-15[L] FedRAMP - PE-15[M] ISO/IEC 27799:2016 11.1.4 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PE-13 MARS-E v2.2 - PE-15 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 R4 PE-13[HML]{0} NIST SP 800-53 R4 PE-15[HML]{0} NIST SP 800-53 r5 - PE-13 NIST SP 800-53 r5 - PE-15 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-13 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-15

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system, and alert defined personnel or roles (defined in the applicable security plan).

	In the event of a fire, fire detection and suppression devices/systems activate automatically, automatically notify the organization, and automatically notify emergency responders.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization employs fire detection devices/systems for the information system that activate automatically and notify service provider building maintenance/physical security personnel and service provider emergency responders with incident response responsibilities in the event of a fire.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	In the event of a fire, fire detection and suppression devices/systems activate automatically, notify organization-specified personnel, and notify emergency responders.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization employs a penetration testing process that includes attempts to bypass or circumvent controls associated with physical access points to the facility.

Control Reference: 08.e Working in Secure Areas

Control Specification:	Physical protection and guidelines for working in secure areas shall be designed and applied.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The arrangements for working in secure areas include controls for the employees, contractors, and third-party users working in the secure area, as well as other third-party activities taking place there. Personnel are aware of the existence of, or activities within, a secure area on a need to know basis.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) ISO/IEC 27002:2022 - 7(6) ISO/IEC 27799:2016 11.1.5
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	

Level 2 Implementation (example):	Unsupervised personnel working in secure areas is avoided both for safety reasons and to prevent opportunities for malicious activities. Vacant secure areas are physically locked and periodically checked. Photographic, video, audio, or other recording equipment such as cameras in mobile devices are not allowed unless otherwise authorized.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) ISO/IEC 27799:2016 11.1.5

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	The organization ensures all computers, electronic media, and removable media containing FTI, are kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

Control Reference: 08.f Public Access, Delivery, and Loading Areas

Control Specification:	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	Access to a delivery and loading area from outside of the building is restricted to identified and authorized personnel. The external doors of a delivery and loading area are secured when the internal doors are opened.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-16 (HIGH; MOD) ISO/IEC 27799:2016 11.1.6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records

Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The delivery and loading area is designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building. Incoming material is registered in accordance with asset management procedures on entry to the site. Incoming and outgoing shipments are physically segregated, where possible.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-16 (HIGH; MOD) ISO/IEC 27799:2016 11.1.6 NIST Cybersecurity Framework v1.1 - PR.IP-5

Objective Name: 08.02 Equipment Security

Control Objective:	To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities.

Control Reference: 08.g Equipment Siting and Protection

Control Specification:	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental
Level 1 Implementation (example):	The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, and considers the physical and environmental hazards in its risk mitigation strategy.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) HITRUST De-ID Framework - De-ID Framework v1 Physical and Environmental Security: General HITRUST De-ID Framework - De-ID Framework v1 Physical Security: General ISO/IEC 27002:2022 - 7(5) NIST SP 800-53 R4 PE-18(1)[S]{0} NIST SP 800-53 r5 - PE-23

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Supplemental
Level 2 Implementation (example):	Guidelines for eating, drinking, and smoking in proximity to information assets are established. Lightning protection is applied to all buildings. Lightning protection filters (e.g., surge protectors) are fitted to all incoming power and communications lines.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.2 AICPA Trust Services Criteria - AICPA 2017 CC6.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-14 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-18 (HIGH) FedRAMP - PE-14(2)[H] FedRAMP - PE-14(2)[M] FedRAMP - PE-15[L] FedRAMP - PE-18[H] Health Industry Cybersecurity Practices - 2.M.A HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(c) HIPAA Security Rule - § 164.310(d)(1) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Physical and Environmental Security: General HITRUST De-ID Framework - De-ID Framework v1 Physical Security: General ISO/IEC 27002:2022 - 7(8) ISO/IEC 27799:2016 11.1.4 ISO/IEC 27799:2016 11.2.1 NIST Cybersecurity Framework v1.1 - DE.CM-2 NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST Cybersecurity Framework v1.1 - PR.DS-8 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 R4 PE-14(1)[S]{0} NIST SP 800-53 R4 PE-14(2)[S]{0} NIST SP 800-53 R4 PE-18[H]{1} NIST SP 800-53 R4 PE-18[H]{2} NIST SP 800-53 R4 PE-19(1)[S]{0} NIST SP 800-53 R4 PE-19[S]{2} NIST SP 800-53 R4 PE-9(2)[S]{2} NIST SP 800-53 R4 SC-28(2)[S]{0} NIST SP 800-53 R4 SC-40(1)[S]{0} NIST SP 800-53 r5 - PE-14(1) NIST SP 800-53 r5 - PE-14(2) NIST SP 800-53 r5 - PE-18 NIST SP 800-53 r5 - PE-19 NIST SP 800-53 r5 - PE-19(1) NIST SP 800-53 r5 - PE-21 NIST SP 800-53 r5 - SC-28(2) NIST SP 800-53 r5 - SC-40(1) NY OHIP Moderate-Plus Security Baseline v5.0 - PE-18 PCI DSS v3.2.1 9.1.3 PCI DSS v3.2.1 9.9 PCI DSS v3.2.1 9.9.2 Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(j)
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The service provider measures temperature at server inlets and humidity levels by dew point.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Multifunction Devices (MFDs) are locked with a mechanism to prevent physical access to the hard disk. Fax machines are placed in a secured area.

Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization periodically inspects payment card device surfaces to detect tampering (for example, addition of card skimmers to devices) or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	When sending or receiving faxes containing PII: fax machines are located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions, or fax machines must be located in a secured area; accurate broadcast lists and other preset numbers of frequent fax recipients are maintained; and a cover sheet is used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Control Reference: 08.h Supporting Utilities

Control Specification:	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	High Moderate
Level 1 Implementation (example):	An uninterruptable power supply (UPS) to support orderly close down is required for equipment supporting critical business operations. Power contingency plans cover the action to be taken on failure of the UPS. The organization ensures UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer’s recommendations.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 A1.2 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-11(01) (HIGH) FedRAMP - PE-11[H] FedRAMP - PE-11[M] ISO/IEC 27002:2022 - 7(11) ISO/IEC 27799:2016 11.2.2 MARS-E v2.2 - PE-11 NIST Cybersecurity Framework v1.1 - ID.BE-4 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST Cybersecurity Framework v1.1 - PR.PT-5 NIST SP 800-53 R4 PE-11[HM]{0} NIST SP 800-53 r5 - PE-11

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning are adequate for the systems they are supporting. Support utilities are regularly inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. The organization maintains temperature and humidity levels in facilities where critical information processing systems reside within acceptable vendor-recommended levels. The organization monitors these levels at an organization-defined frequency.

Level 2 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-10 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-12 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-14 (HIGH; MOD) FedRAMP - PE-10a[H] FedRAMP - PE-10a[M] FedRAMP - PE-10b[H] FedRAMP - PE-10b[M] FedRAMP - PE-10c[H] FedRAMP - PE-10c[M] FedRAMP - PE-12[H] FedRAMP - PE-12[L] FedRAMP - PE-12[M] ISO/IEC 27799:2016 11.2.1 ISO/IEC 27799:2016 11.2.2 ISO/IEC 27799:2016 11.2.4 MARS-E v2.2 - PE-10a MARS-E v2.2 - PE-10b MARS-E v2.2 - PE-10c MARS-E v2.2 - PE-12 MARS-E v2.2 - PE-14a MARS-E v2.2 - PE-14b MARS-E v2.2 - PE-15 MARS-E v2.2 - PE-9 NIST Cybersecurity Framework v1.1 - ID.BE-4 NIST Cybersecurity Framework v1.1 - PR.IP-5 NIST SP 800-53 R4 PE-10a[HM]{0} NIST SP 800-53 R4 PE-10b[HM]{0} NIST SP 800-53 R4 PE-10c[HM]{0} NIST SP 800-53 R4 PE-12(1)[S]{0} NIST SP 800-53 R4 PE-12[HML]{0} NIST SP 800-53 R4 PE-14[HML]{0} NIST SP 800-53 r5 - PE-10 NIST SP 800-53 r5 - PE-12 NIST SP 800-53 r5 - PE-12(1) NIST SP 800-53 r5 - PE-14 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-10[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-10a NY OHIP Moderate-Plus Security Baseline v5.0 - PE-10b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-10c NY OHIP Moderate-Plus Security Baseline v5.0 - PE-12 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-14[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-14[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-14[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-14a NY OHIP Moderate-Plus Security Baseline v5.0 - PE-14b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-9[IS.1]

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records

Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation (example):	Voice services are adequate to meet local legal requirements for emergency communications.
Level 3 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-08 (HIGH; MOD) ISO/IEC 27799:2016 11.2.2 NIST Cybersecurity Framework v1.1 - ID.BE-4
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization provides a long-term alternate power supply (e.g., uninterruptable power supply (UPS), generator, backup power source) for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization continuously monitors and maintains both temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments; and Requirements.
Level Providers Implementation Requirements	
Level Providers Implementation (example):	Backup generators, multiple power sources and/or separate substations are implemented based on the level of the organization: Level 1 Providers: A back-up generator is considered if processing is required to continue in case of a prolonged power failure; Level 1 Providers: An adequate supply of fuel is available to ensure that the generator, if used, can perform for a prolonged period; Level 2 Providers: A back-up generator is implemented; Level 2 Providers: An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period; Level 2 Providers: Generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations; Level 3 Providers: Multiple power sources or a separate power substation be used; Level 3 Providers: Telecommunications equipment are connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services; Level 3 Providers: The organization develops telecommunications service agreements that contain priority of service (Telecommunications Service Priority) provisions.
Level HIPAA Implementation Requirements	
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization has a suitable electrical supply that conforms to the equipment manufacturer's specifications.

Control Reference: 08.i Cabling Security

Control Specification:	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	High Moderate Supplemental
Level 1 Implementation (example):	The organization protects power equipment and power cabling for the information system from damage and destruction.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-09 (HIGH; MOD) FedRAMP - PE-9[H] FedRAMP - PE-9[M] ISO/IEC 27002:2022 - 7(12) ISO/IEC 27799:2016 11.2.3 MARS-E v2.2 - PE-9 NIST SP 800-53 R4 PE-9(2)[S]{1} NIST SP 800-53 R4 PE-9[HM]{0} NIST SP 800-53 r5 - PE-9 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-9
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 2 Implementation (example):	Access to patch panels and cable rooms are controlled. The organization ensures a documented patch list, clearly identifiable cable, and equipment markings are used to minimize handling errors, such as accidental patching of wrong network cables. The organization ensures power and telecommunications lines into information processing facilities are underground, where possible, or subject to adequate alternative protection.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-09 (HIGH; MOD) FedRAMP - PE-4[H] FedRAMP - PE-4[M] Health Industry Cybersecurity Practices - 6.S.B HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(c) IRS Pub 1075 - PE-4 ISO/IEC 27002:2022 - 7(12) ISO/IEC 27799:2016 11.2.3 MARS-E v2.2 - PE-4 NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-53 R4 PE-19[S]{1} NIST SP 800-53 R4 PE-3(1)[H]{0} NIST SP 800-53 R4 PE-3(5)[S]{1} NIST SP 800-53 R4 PE-3(5)[S]{2} NIST SP 800-53 R4 PE-4[HM]{0} NIST SP 800-53 R4 SC-37(1)[S]{1} NIST SP 800-53 R4 SC-37[S]{0} NIST SP 800-53 r5 - PE-19 NIST SP 800-53 r5 - PE-3(5) NIST SP 800-53 r5 - PE-4 NIST SP 800-53 r5 - SC-37 NIST SP 800-53 r5 - SC-37(1) NY OHIP Moderate-Plus Security Baseline v5.0 - PE-4 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-4[IS.1] PCI DSS v3.2.1 9.1.2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation (example):	The organization ensures technical sweeps and physical inspections are initiated for unauthorized devices being attached to the cables.
Level 3 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-08(03) (HIGH; MOD) ISO/IEC 27799:2016 11.2.3
Level FTI Custodians Implementation Requirements	

Control Reference: 08.j Equipment Maintenance	
Control Specification:	Equipment shall be correctly maintained to ensure its continued availability and integrity.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization formally addresses purpose, scope, roles associated with, responsibilities associated with, management's commitment to, coordination among organizational entities associated with, and compliance with the organization's equipment maintenance program. Formal, documented procedures exist to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC3.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-01 (HIGH; MOD) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) ISO/IEC 27002:2022 - 7(13) Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.MA-1 Veterans Affairs Cybersecurity Program Directive 6500 - b(6)(a)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Texas Medical Records Privacy Act High Low Moderate Supplemental

Level 2 Implementation (example):	Equipment is maintained in accordance with the supplier's recommended service intervals and specifications, insurance policies, and the organization's maintenance program. The organization ensures only authorized maintenance personnel carry out repairs and service the equipment. Appropriate controls are implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization. The organization establishes a process for maintenance personnel authorization, maintains a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-05(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-06 (HIGH; MOD) FedRAMP - MA-5a[H] FedRAMP - MA-5a[L] FedRAMP - MA-5a[M] FedRAMP - MA-5b[H] FedRAMP - MA-5b[L] FedRAMP - MA-5b[M] FedRAMP - MA-5c[H] FedRAMP - MA-5c[L] FedRAMP - MA-5c[M] FedRAMP - MA-6[H] FedRAMP - MA-6[M] HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.310(a)(2)(iv) IRS Pub 1075 - 2.B.3.3(8)a IRS Pub 1075 - 2.B.3.3(8)b IRS Pub 1075 - CM-4(2) IRS Pub 1075 - MA-2e IRS Pub 1075 - MA-2f1 IRS Pub 1075 - MA-2f2 IRS Pub 1075 - MA-2f3 IRS Pub 1075 - MA-2f4 IRS Pub 1075 - MA-2f5 IRS Pub 1075 - MA-5(5) IRS Pub 1075 - MA-5a IRS Pub 1075 - MA-5b IRS Pub 1075 - MA-5c IRS Pub 1075 - MA-6 IRS Pub 1075 - SR-11(2) ISO/IEC 27002:2022 - 7(13) ISO/IEC 27799:2016 11.2.4 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - MA-4a MARS-E v2.2 - MA-4b MARS-E v2.2 - MA-4c MARS-E v2.2 - MA-4d MARS-E v2.2 - MA-5a MARS-E v2.2 - MA-5b MARS-E v2.2 - MA-5c MARS-E v2.2 - MA-6 NIST Cybersecurity Framework v1.1 - PR.MA-1 NIST SP 800-171 r2 - 3.7.1[a] NIST SP 800-171 r2 - 3.7.2[a] NIST SP 800-171 r2 - 3.7.2[b] NIST SP 800-171 r2 - 3.7.2[c] NIST SP 800-171 r2 - 3.7.2[d] NIST SP 800-171 r2 - 3.7.3[a] NIST SP 800-171 r2 - 3.7.6[a] NIST SP 800-53 R4 MA-4(5)a[S]{0}

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 R4 MA-4(5)b[S]{1} NIST SP 800-53 R4 MA-4a[HML]{0} NIST SP 800-53 R4 MA-5(2)[S]{1} NIST SP 800-53 R4 MA-5(4)[S]{2} NIST SP 800-53 R4 MA-5[HML]{0} NIST SP 800-53 R4 MA-6(1)[S]{0} NIST SP 800-53 R4 MA-6(2)[S]{0} NIST SP 800-53 R4 MA-6[HM]{0} NIST SP 800-53 r5 - MA-4(5)a NIST SP 800-53 r5 - MA-4(5)b NIST SP 800-53 r5 - MA-4a NIST SP 800-53 r5 - MA-5 NIST SP 800-53 r5 - MA-5(2) NIST SP 800-53 r5 - MA-5(4) NIST SP 800-53 r5 - MA-6 NIST SP 800-53 r5 - MA-6(1) NIST SP 800-53 r5 - MA-6(2) NIST SP 800-53 r5 - MA-7 NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4a NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4b NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4c NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4d NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4e NY OHIP Moderate-Plus Security Baseline v5.0 - MA-5[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - MA-5[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - MA-5[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - MA-5a NY OHIP Moderate-Plus Security Baseline v5.0 - MA-5b NY OHIP Moderate-Plus Security Baseline v5.0 - MA-5c NY OHIP Moderate-Plus Security Baseline v5.0 - MA-6 NY OHIP Moderate-Plus Security Baseline v5.0 - MA-6[IS.1]
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High) High Low Moderate
Level 3 Implementation (example):	The organization approves, controls and monitors the use of information system maintenance tools (e.g., hardware and software brought into the organization for diagnostic/repair actions). All maintenance tools carried into the facility by maintenance personnel are inspected for improper or unauthorized modifications.

	All media containing diagnostic and test programs are checked for malicious code prior to the media being used in the information system.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-03(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-03(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MA-04(02) (HIGH; MOD) FedRAMP - MA-3 (1)[H] FedRAMP - MA-3 (1)[M] FedRAMP - MA-3 (2)[H] FedRAMP - MA-3 (2)[M] FedRAMP - MA-3[H] FedRAMP - MA-3[M] FedRAMP - MA-4 (2)[H] FedRAMP - MA-4 (2)[M] FedRAMP - MA-4b[H] FedRAMP - MA-4b[L] FedRAMP - MA-4b[M] HIPAA Security Rule - § 164.308(a)(5)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.310(a)(2)(iv) IRS Pub 1075 - MA-3(1) IRS Pub 1075 - MA-3(2) IRS Pub 1075 - MA-3(4) IRS Pub 1075 - MA-3(5) IRS Pub 1075 - MA-3a IRS Pub 1075 - MA-4b MARS-E v2.2 - MA-3 MARS-E v2.2 - MA-3(1) MARS-E v2.2 - MA-3(2) MARS-E v2.2 - MA-4(2) NIST Cybersecurity Framework v1.1 - DE.CM-4 NIST Cybersecurity Framework v1.1 - PR.MA-1 NIST Cybersecurity Framework v1.1 - PR.MA-2 NIST SP 800-171 r2 - 3.7.4[a] NIST SP 800-53 R4 MA-3(1)[HM]{0} NIST SP 800-53 R4 MA-3(2)[HM]{0} NIST SP 800-53 R4 MA-3[HM]{0} NIST SP 800-53 R4 MA-4(2)[HM]{0} NIST SP 800-53 R4 MA-4b[HML]{0} NIST SP 800-53 r5 - MA-3 NIST SP 800-53 r5 - MA-3(1) NIST SP 800-53 r5 - MA-3(2) NIST SP 800-53 r5 - MA-3(5) NIST SP 800-53 r5 - MA-4b NY OHIP Moderate-Plus Security Baseline v5.0 - MA-3(1) NY OHIP Moderate-Plus Security Baseline v5.0 - MA-3(1)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - MA-3(2) NY OHIP Moderate-Plus Security Baseline v5.0 - MA-3(2)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - MA-3a
Level CMS Implementation Requirements	
Level CMS Implementation (example):	If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service. The organization audits non-local maintenance and diagnostic sessions using available auditable events and reviews the maintenance records of the sessions.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	Equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the control of the organization, is destroyed, or an exemption is obtained from the information owner explicitly authorizing removal of the equipment from the facility. The organization monitors and approves non-local maintenance and diagnostic activities. When non-local maintenance is completed, the organization terminates the session and network connection.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization reviews previously approved system maintenance tools on at least an annual basis.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: verifying there is no organizational information contained on the equipment; sanitizing or destroying the equipment; retaining the equipment within the facility; or obtaining a written exemption from the CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization: schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on-site or removed to another location; requires that the applicable Business Owner (or an official designated in the applicable security plan) explicitly approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records. The organization reviews previously approved system maintenance tools every 30 days.

Control Reference: 08.k Security of Equipment Off-Premises	
Control Specification:	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization’s premises.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	

Level 1 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	Regardless of ownership, the use of any information processing equipment outside the organization's premises, including equipment used by remote workers, even where such use is permanent (e.g., a core feature of the employee's role), is authorized by management.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) HIPAA Security Rule - § 164.310(a)(1) ISO/IEC 27799:2016 11.2.6
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The organization ensures that equipment and media taken off the premises are not to be left unattended in public places. Portable computers are carried as hand luggage and disguised where possible when travelling. Manufacturers' instructions for protecting equipment are observed at all times (e.g., protection against exposure to strong electromagnetic fields). Home-working controls are applied, including lockable filing cabinets, clear desk policy, and access controls for computers and secure communication with the office.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-17 (HIGH; MOD) HIPAA Security Rule - § 164.310(d)(1) IRS Pub 1075 - 2.C.7(3) IRS Pub 1075 - 2.C.7(4) ISO/IEC 27002:2022 - 7(9) ISO/IEC 27799:2016 11.2.6 ISO/IEC 27799:2016 6.2 ISO/IEC 27799:2016 6.2.1 ISO/IEC 27799:2016 6.2.2 NIST Cybersecurity Framework v1.1 - PR.PT-2

Control Reference: 08.l Secure Disposal or Re-Use of Equipment

Control Specification:	All items of equipment containing storage media shall be checked to ensure that any covered information and licensed software has been removed or securely overwritten prior to disposal.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework The Joint Commission v2016 PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information
Level 1 Implementation (example):	The organization ensures that surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06 (HIGH; MOD) COBIT 5 DS11.4 COBIT 5 DSS05.03 COBIT 5 DSS05.06 Health Industry Cybersecurity Practices - 5.M.C Health Industry Cybersecurity Practices - 5.M.D HIPAA Security Rule - § 164.310(d)(2)(iii) HITRUST De-ID Framework - De-ID Framework v1 Disposal: Data Destruction Procedures ISO/IEC 27799:2016 11.2.7 Legacy Inheritance Support - L.I.S. NY OHIP Moderate-Plus Security Baseline v5.0 - MP-4[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-4b OCR Guidance for Unsecured PHI (2)(ii) PCI DSS v3.2.1 9.8.1 The Joint Commission (v2016) - TJC IM.02.01.03, EP 7

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FISMA HITRUST De-ID Framework The Joint Commission v2016 PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information Supplemental

Level 2 Implementation (example):	The organization: ensures disk wiping or degaussing is used to securely remove electronic information; ensures shredding, disintegration, grinding surfaces, incineration, pulverization, or melting are used to destroy electronic and hard copy media; ensures devices containing covered and/or confidential information are physically destroyed or the information is destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function; renders information unusable, unreadable, or indecipherable on digital system media prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; renders information unusable, unreadable, or indecipherable on non-digital system media prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; destroys media containing covered and/or confidential information that cannot be sanitized.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.13 AICPA Trust Services Criteria - AICPA 2017 CC6.5 Banking Requirements - FFIEC IS v2016 A.6.16(e) Banking Requirements - FFIEC IS v2016 A.6.18(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06 (HIGH; MOD) COBIT 5 DS1.4 COBIT 5 DS11.4 COBIT 5 DS11.6 COBIT 5 DSS05.03 COBIT 5 DSS05.06 FedRAMP - MP-6a[H] FedRAMP - MP-6a[L] FedRAMP - MP-6a[M] FedRAMP - MP-6b[H] FedRAMP - MP-6b[L] FedRAMP - MP-6b[M] Health Industry Cybersecurity Practices - 5.M.D Health Industry Cybersecurity Practices - 5.S.C Health Industry Cybersecurity Practices - 9.M.D HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(i) HIPAA Security Rule - § 164.310(d)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Disposal: Data Destruction Procedures IRS Pub 1075 - MP-6a IRS Pub 1075 - MP-6b ISO/IEC 27002:2022 - 7(14) ISO/IEC 27799:2016 11.2.7 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - MP-6a MARS-E v2.2 - MP-6b MARS-E v2.2 - MP-6c NIST Cybersecurity Framework v1.1 - PR.IP-6 NIST SP 800-171 r2 - 3.8.3[a] NIST SP 800-171 r2 - 3.8.3[b] NIST SP 800-53 R4 MP-8[S]{4} NIST SP 800-53 r5 - MP-8 NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6[PRIV.1] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6[PRIV.2] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6[PRIV.3] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6a NY OHIP Moderate-Plus Security Baseline v5.0 - MP-6b OCR Guidance for Unsecured PHI (2)(i) OCR Guidance for Unsecured PHI (2)(ii) PCI DSS v3.2.1 9.8.1 PCI DSS v3.2.1 9.8.2 The Joint Commission (v2016) - TJC IM.02.01.03, EP 7 Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(a) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(b) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(e) Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(h)

Level NYDOH Implementation Requirements

Level NYDOH Implementation (example):	The organization ensures the hypervisor enforces sanitization of the instance (container) image file space upon release.

	The organization securely stores surplus equipment while not in use, disposed of, or sanitized in accordance with NIST 800-88 when no longer required.

Control Reference: 08.m Removal of Property	
Control Specification:	Equipment, information or software shall not be taken off site without prior authorization.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA The Joint Commission v2016 CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization ensures equipment, information, and software are not taken off-site without prior authorization. The organization ensures employees, contractors, and third-party users who have authority to permit off-site removal of assets are clearly identified.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-16 (HIGH; MOD) FedRAMP - PE-16[L] FedRAMP - PE-16[M] HIPAA Security Rule - § 164.310(d)(1) IRS Pub 1075 - PE-3(2) ISO/IEC 27799:2016 11.2.5 MARS-E v2.2 - PE-16 NIST SP 800-53 R4 PE-16[HML]{2} NIST SP 800-53 r5 - PE-16 The Joint Commission (v2016) - TJC IM.02.01.03, EP 4
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA The Joint Commission v2016 CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	Time limits for equipment removal are set. Returned equipment is checked for compliance. Equipment are recorded as being removed off-site. Equipment are recorded when returned.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-16 (HIGH; MOD) FedRAMP - PE-16[H] HIPAA Security Rule - § 164.310(d)(1) IRS Pub 1075 - PE-16a IRS Pub 1075 - PE-16b ISO/IEC 27799:2016 11.2.5 MARS-E v2.2 - PE-16 NIST Cybersecurity Framework v1.1 - PR.DS-3 NIST SP 800-53 R4 PE-16[HML]{1} NIST SP 800-53 r5 - PE-16 NY OHIP Moderate-Plus Security Baseline v5.0 - PE-16a

Control Category: 09.0 - Communications and Operations Management

Objective Name: 09.01 Documented Operating Procedures

Control Objective:	To ensure that operating procedures are documented, maintained and made available to all users who need them.

Control Reference: 09.a Documented Operations Procedures

Control Specification:	Operating procedures shall be documented, maintained, and made available to all users who need them.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	Operating procedures and the documented procedures for system activities are treated as formal documents. Changes to operating procedures and the documented procedures for system activities are authorized by management.
Level 1 Authoritative Source Mapping:	21 CFR Part 11.10(k) Banking Requirements - FFIEC IS v2016 A.6.1 HIPAA Security Rule - § 164.316(a) ISO/IEC 27002:2022 - 5(37) ISO/IEC 27799:2016 12.1.1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	

Level 2 Regulatory Factors:	FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	The organization prepares documented procedures for system activities associated with information and communication assets, including computer start-up, computer close-down procedures, backup of data, equipment maintenance, media handling, electronic communications, computer room management, mail handling management, and safety. The detailed instructions for the execution of each job in its operating procedures include: processing and handling of information; the backup of data; scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times; instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities; support contacts in the event of unexpected operational or technical difficulties; special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs; system restart and recovery in the event of system failure; and the management of audit-trail and system log information.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(k) Banking Requirements - FFIEC IS v2016 A.6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AT-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) ISO/IEC 27799:2016 12.1.1 NIST Cybersecurity Framework v1.1 - DE.AE-1 NIST Cybersecurity Framework v1.1 - PR.PT-1 NIST SP 800-53 R4 AU-15[S]{0} NIST SP 800-53 R4 SI-7(16)[S]{0} NIST SP 800-53 r5 - SI-7(16) PCI DSS v3.2.1 1.5 PCI DSS v3.2.1 10.9 PCI DSS v3.2.1 11.6 PCI DSS v3.2.1 2.5 PCI DSS v3.2.1 3.7 PCI DSS v3.2.1 4.3 PCI DSS v3.2.1 5.4 PCI DSS v3.2.1 6.7 PCI DSS v3.2.1 7.3 PCI DSS v3.2.1 8.8 PCI DSS v3.2.1 9.10

Level FTI Custodians Implementation Requirements	

Level PCI Implementation Requirements	
Level PCI Implementation (example):	Operational procedures are documented, communicated, and in use for: managing firewalls; managing vendor defaults and other security parameters; protecting stored cardholder data; encrypting transmissions of cardholder data; protecting systems against malware; developing and maintaining secure systems and applications; restricting access to cardholder data; identification and authentication; restricting physical access to cardholder data; monitoring access to network resources and cardholder data; and security monitoring and testing.

Control Reference: 09.b Change Management

Control Specification:	Changes to information assets and systems shall be controlled and archived.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.
Level 1 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 6.M.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 7.M.D Health Industry Cybersecurity Practices - 9.M.A ISO/IEC 27002:2022 - 8(32) NIST SP 800-171 r2 - 3.4.3[a] NIST SP 800-171 r2 - 3.4.3[b] NIST SP 800-171 r2 - 3.4.3[c] NIST SP 800-171 r2 - 3.4.3[d]

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements Supplemental Requirements CMS Minimum Security Requirements (High) Supplemental

Level 2 Implementation (example):	Changes to information assets, including systems, networks, and network services, are controlled and archived. Changes are managed strictly and consistently. Further, formal management responsibilities and procedures are in place to ensure satisfactory control of all changes to equipment, software or procedures, including: the identification and recording of significant changes; the planning and testing of changes; the assessment of the potential impacts, including security impacts, of such changes; the formal approval for proposed changes; and the communication of change details to all relevant persons.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.11 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(7)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) ISO/IEC 27799:2016 12.1.2 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - RC.RP-1 NIST SP 800-171 r2 - 3.4.3[a] NIST SP 800-171 r2 - 3.4.3[d] NIST SP 800-53 R4 CM-5(6)[S]{2} NIST SP 800-53 r5 - CM-5(6) Supplemental Requirements - SR v6.4 27-1 Supplemental Requirements - SR v6.4 27-2 Supplemental Requirements - SR v6.4 7b.4-0
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization maintains a baseline configuration for information system development, and a test environment that is managed separately from the operational baseline configuration. The organization retains records of configuration-controlled changes to the information system for a minimum of three years after the change.
Level DGF Implementation Requirements	
Level DGF Implementation (example):	Data Governance tools and technologies are tested and approved for interoperability.

Control Reference: 09.c Segregation of Duties

Control Specification:	Separation of duties shall be enforced to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	Banking Requirements High Low Moderate Supplemental
Level 1 Implementation (example):	Access authorization (e.g., access requests, approvals, and provisioning) is segregated among multiple individuals or groups.
Level 1 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.8(c) Health Industry Cybersecurity Practices - 3.M.B HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) ISO/IEC 27799:2016 9.1.1 ISO/IEC 27799:2016 9.2.1 NIST Cybersecurity Framework v1.1 - PR.AC-4 NIST SP 800-53 R4 AC-2i[HML]{1} NIST SP 800-53 R4 AC-3(2)[S]{1} NIST SP 800-53 r5 - AC-2e NIST SP 800-53 r5 - AC-2i1 NIST SP 800-53 r5 - AC-3(2)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	FISMA Supplemental Requirements High Moderate Supplemental
Level 2 Implementation (example):	Separation of duties, or the monitoring of activities, audit trails, management supervision, or a system of dual control when segregation is not possible, is used to limit the risk of unauthorized or unintentional modification of information assets. No single person is able to access, modify, or use information assets without authorization or detection.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC1.3 AICPA Trust Services Criteria - AICPA 2017 CC3.3 AICPA Trust Services Criteria - AICPA 2017 CC5.1 AICPA Trust Services Criteria - AICPA 2017 CC6.3 Banking Requirements - FFIEC IS v2016 A.6.8(d) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-05 (HIGH; MOD) COBIT 5 DS05.04 COBIT 5 DS5.5 COBIT 5 DS5.7 FedRAMP - AC-5a[H] FedRAMP - AC-5a[M] FedRAMP - AC-5b[H] FedRAMP - AC-5b[M] FedRAMP - AC-5c[H] FedRAMP - AC-5c[M] Health Industry Cybersecurity Practices - 3.L.C HIPAA Privacy Rule - 164.504(f)(2)(ii)(J) HIPAA Security Rule - § 164.308(a)(3)(ii)(A) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) IRS Pub 1075 - AC-5a IRS Pub 1075 - AC-5b ISO/IEC 27002:2022 - 5(3) ISO/IEC 27799:2016 6.1.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-5a MARS-E v2.2 - AC-5b MARS-E v2.2 - AC-5c NIST Cybersecurity Framework v1.1 - DE.DP-1 NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST SP 800-171 r2 - 3.1.4[a] NIST SP 800-171 r2 - 3.1.4[b] NIST SP 800-171 r2 - 3.1.4[c] NIST SP 800-53 R4 AC-3(2)[S]{2} NIST SP 800-53 R4 AC-5[HM]{0} NIST SP 800-53 R4 CM-9(1)[S]{0} NIST SP 800-53 R4 SA-11(3)a[S]{1} NIST SP 800-53 R4 SC-3(4)[S]{0} NIST SP 800-53 r5 - AC-3(2) NIST SP 800-53 r5 - AC-5 NIST SP 800-53 r5 - CM-9(1) NIST SP 800-53 r5 - SA-11(3)a NIST SP 800-53 r5 - SA-8(4) NIST SP 800-53 r5 - SC-3(4) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-5a NY OHIP Moderate-Plus Security Baseline v5.0 - AC-5b Supplemental Requirements - SR v6.4 7b.2-0 Veterans Affairs Cybersecurity Program Directive 6500 - b(1)(f)

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 3 Regulatory Factors:	FedRAMP Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	The number of administrators is limited to the minimum necessary based upon each users' role and responsibilities. Security personnel responsible for administering access controls do not perform audit functions for these controls. Development, testing, quality assurance and production functions are divided among separate individuals or groups to ensure independence.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.8(d) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-05 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 ISO/IEC 27002:2022 - 8(31) ISO/IEC 27799:2016 6.1.2 MARS-E v2.2 - AC-5a NIST SP 800-53 R4 AC-2i[HML]{2} NIST SP 800-53 R4 AC-4(17)[S]{0} NIST SP 800-53 r5 - AC-25 NIST SP 800-53 r5 - AC-2i2 NIST SP 800-53 r5 - AC-4(17) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-5[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-5[IS.4] PCI DSS v3.2.1 6.4.2
Level FTI Custodians Implementation Requirements	

Control Reference: 09.d Separation of Development, Test, and Operational Environments

Control Specification:	Development, test, and operational environments shall be separated and controlled to reduce the risks of unauthorized access or changes to the operational system.
Factor Type:	System

Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Supplemental Requirements
Level 1 Implementation (example):	The organization ensures separation between production and non-production (development, test/quality assurance) environments is established and controls are implemented to prevent operational issues.
Level 1 Authoritative Source Mapping:	ISO/IEC 27002:2022 - 8(25) ISO/IEC 27002:2022 - 8(31) Supplemental Requirements - SR v6.4 26.1-0
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	Information systems audit tools (e.g., software or data files) are separated from development and operational systems. The organization minimizes any testing on production systems. When testing must be performed, a test plan is developed that documents all changes to the system, and the procedures for undoing any changes made to the system (e.g., removing test accounts).

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 18.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02 (HIGH; MOD) ISO/IEC 27799:2016 12.1.2 ISO/IEC 27799:2016 12.1.4 NIST SP 800-53 r5 - SA-3(2)a PCI DSS v3.2.1 6.3.1 PCI DSS v3.2.1 6.3.2 PCI DSS v3.2.1 6.4.1 PCI DSS v3.2.1 6.4.3 PCI DSS v3.2.1 6.4.4

Level CMS Implementation Requirements

Level CMS Implementation (example):	The organization ensures all systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, is restricted by source and destination access control lists (ACLs), is restricted by ports, and is restricted by protocols.

Level FTI Custodians Implementation Requirements

Level HIX Implementation Requirements

Level Supplemental Requirements Implementation Requirements

Objective Name: 09.02 Control Third Party Service Delivery

Control Objective:	To ensure that third party service providers maintain security requirements and levels of service as part of their service delivery agreements.

Control Reference: 09.e Service Delivery

Control Specification:	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	HITRUST De-ID Framework Texas Medical Records Privacy Act

Level 1 Implementation (example):	Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions (e.g., reliability, availability, and response times for the provision of services), security controls, and other aspects of services management (e.g., monitoring, auditing, impacts to the organization's resilience, and change management).
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 23 NYCRR 500 - 500.02(c) 23 NYCRR 500 - 500.11(a)(1) 23 NYCRR 500 - 500.11(a)(2) 23 NYCRR 500 - 500.11(a)(3) 23 NYCRR 500 - 500.11(b)(3) 23 NYCRR 500 - 500.11(b)(4) Banking Requirements - FFIEC IS v2016 A.6.31(c) Banking Requirements - FFIEC IS v2016 A.6.31(g) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) EU GDPR Article 32(4) IRS Pub 1075 - 2.C.9(1)a IRS Pub 1075 - 2.C.9(1)e IRS Pub 1075 - 2.C.9(1)f ISO/IEC 27799:2016 15.1.1 NIST Cybersecurity Framework v1.1 - DE.CM-6 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(f)(2)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	The organization develops, disseminates, and reviews/updates annually a list of current service providers, which includes a description of services provided. In the case of outsourcing arrangements, the organization plans the necessary transitions (of information, information processing systems, and anything else that needs to be moved), and ensures that security is maintained throughout the transition period. The organization ensures that the third-party maintains sufficient service capabilities together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC9.2 Banking Requirements - FFIEC IS v2016 A.6.31(a) Banking Requirements - FFIEC IS v2016 A.6.31(g) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) FedRAMP - SA-9(5)[M] FTC Red Flags Rule (16 CFR 681) - 681.A6.c HIPAA Privacy Rule - 164.504(e)(2)(ii)(B) HIPAA Privacy Rule - 164.530(f) HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(3)(i) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.312(a)(1) HIPAA Security Rule - § 164.312(c)(1) ISO/IEC 27799:2016 15.2.1 MARS-E v2.2 - SC-32 NIST Cybersecurity Framework v1.1 - DE.CM-6 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-53 R4 SA-9(5)[S]{0} NIST SP 800-53 r5 - SA-9(5) NIST SP 800-53 r5 - SA-9(8) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-1[PRIV.2] NY OHIP Moderate-Plus Security Baseline v5.0 - SA-9(5) Ontario Personal Health Information Protection Act - 14(2)(a) Ontario Personal Health Information Protection Act - 14(2)(b) Ontario Personal Health Information Protection Act - 14(2)(c) Ontario Personal Health Information Protection Act - 14(2)(d) PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.1 PCI DSS v3.2.1 2.6 Supplemental Requirements - SR v6.4 45a-2
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization ensures notification of the intent to outsource information system services outside the continental U.S. is sent to CMS at least 60 days prior to commitment of the outsourcing.
Level De-ID Data Environment Implementation Requirements	
Level De-ID Data Environment Implementation (example):	The organization ensures that de-identified data is not accessed from offshore; nor is such data received, stored, processed, or disposed via information technology systems located offshore. Otherwise, the organization justifies the offshore disclosure.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization restricts the location of information processing, information/data, and information system services to U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction for all High impact data, systems, or services.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization ensures that information systems that receive, process, store, access, protect and/or transmit FTI must be located, operated, and accessed within the United States. When a contract developer is used, the organization documents, through contract requirements, that all FTI systems (i.e., beyond commercial products used as components) are located within the United States and are developed physically within the United States by United States citizens or those with lawful resident status.

	FTI may not be accessed by organization employees, agents, representatives, or contractors located off-shore, outside of the United States, or its territories. FTI may not be received, stored, processed, or disposed via information technology systems located off-shore.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization: Notifies CMS of plans to outsource information system services prior to the awarding of a contract; Requires that providers of external information system services comply with organizational security requirements (consistent with 45 CFR 155.260(b)), define security and privacy roles and responsibilities in the service contract or agreement, and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; Defines and documents oversight and user roles and responsibilities with regard to external information system services; Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance; Employs defined process, methods, and techniques (defined in the applicable security plan) to monitor security and privacy control compliance by external service providers on an ongoing basis; and Notifies CMS at least five days prior to transmitting data into an external information service environment. The outsourcing of information system services outside the continental U.S. is authorized by the CIO of CMS. The service contract or agreement must include language requiring the provider to be subject to U.S. Federal laws and regulations protecting personally identifiable information. Depending on the outcome of the risk assessment, the organization restricts the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization executes a master service agreement with a third-party service provider experienced in incident response and forensics on a contingency basis. The organization ensures that service contracts for incident management require the service provider to deliver immediate remote support and be on-site (if possible and/or where practical) within 48 hours of an incident.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization defines and documents government oversight and user roles and responsibilities with regard to external information system services.
Control Reference: 09.f Monitoring and Review of Third Party Services	
Control Specification:	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	

Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization ensures a periodic review of service-level agreements (SLAs) is conducted at least annually, and compared against the monitoring records.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.11(a)(4) IRS Pub 1075 - 2.C.9(1)f ISO/IEC 27799:2016 15.2.1 NIST Cybersecurity Framework v1.1 - DE.CM-6 PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.4
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	The organization periodically audits the network services to ensure that network service providers have implemented the required security features, and meet the requirements agreed with management, including new and existing regulations. The organization monitors security control compliance by external service providers on an ongoing basis. Monitoring involves a service management relationship and process between the organization and the third party. The organization monitors the network service features and service levels to detect abnormalities and violations.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.21(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) FedRAMP - SA-9c[H] FedRAMP - SA-9c[L] FedRAMP - SA-9c[M] FTC Red Flags Rule (16 CFR 681) - 681.1e4 FTC Red Flags Rule (16 CFR 681) - 681.A6.c ISO/IEC 27001:2022 - 8.1d ISO/IEC 27799:2016 13.1.2 ISO/IEC 27799:2016 15.2.1 NIST Cybersecurity Framework v1.1 - DE.CM-6 NIST Cybersecurity Framework v1.1 - DE.DP-4 NIST SP 800-53 R4 IR-7(2)a[S]{1} NIST SP 800-53 r5 - IR-7(2)a PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.4 PCI DSS v3.2.1 2.6

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 3 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements CMS Minimum Security Requirements (High)
Level 3 Implementation (example):	The organization ensures service reports produced by the third-parties be reviewed, and regular progress meetings are arranged as required by the agreements. The organization ensures third-party audit trails, records of third-party security events, records of third-party operational problems, records of third-party failures, and records of third-party tracing of faults and disruptions related to service delivery are reviewed. Information about information security incidents are provided to the incident response team. This information is reviewed by the third-party that experienced the incident and the organization which the third-party provides services to as required by the agreements and any supporting guidelines and procedures. Any identified problems are resolved and reviewed by the organization as noted above.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.21(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) FTC Red Flags Rule (16 CFR 681) - 681.1e4 FTC Red Flags Rule (16 CFR 681) - 681.A6.c ISO/IEC 27799:2016 15.2.1 NIST Cybersecurity Framework v1.1 - DE.CM-6 PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.4
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.
Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	The organization ensures all supplier entities performing any in-scope work are contractually obligated to comply with the organization’s security requirements, or requirements that are no less stringent. The use of the organization’s information resources and in-scope information by supplier entities will only be for the performance of in-scope work. A documented program is maintained and adhered to by which supplier entity compliance to the organization’s security requirements is evaluated by supplier and all corrective actions are documented and implemented. The supplier will provide documentation and/or evidence to adequately substantiate such compliance, upon the organization’s request.

Control Reference: 09.g Managing Changes to Third Party Services

Control Specification:	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization ensures that third-party organizations use appropriate change management procedures for any changes to a third-party service or organizational system.
Level 1 Authoritative Source Mapping:	ISO/IEC 27799:2016 15.2.2 NIST Cybersecurity Framework v1.1 - ID.BE-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FTC Red Flags Rule (16 CFR 681)
Level 2 Implementation (example):	The change management on a third-party service includes an assessment and explicit recording of the potential impacts, including security impacts, of such change. Third-party changes are evaluated prior to implementation. Evaluation of third-party changes includes evaluating and implementing changes made by the organization for enhancements made to the current services offered, newly developed applications and systems, modifications or updates of the organization's policies and procedures, and new controls to resolve information security incidents and to improve security. Evaluation of third-party changes includes evaluating and implementing changes in third-party services for changes and enhancement to networks, use of new technologies, adoption of new products or newer versions/releases, new development tools and environments, and changes to physical location.
Level 2 Authoritative Source Mapping:	ISO/IEC 27001:2022 - 8.1d ISO/IEC 27799:2016 15.2.2 NIST Cybersecurity Framework v1.1 - ID.BE-1 NIST Cybersecurity Framework v1.1 - ID.SC-3

Objective Name: 09.03 System Planning and Acceptance

Control Objective:	To ensure that systems meet the businesses current and projected needs to minimize failures.

Control Reference: 09.h Capacity Management

Control Specification:	The availability of adequate capacity and resources shall be planned, prepared, and managed to deliver the required system performance. Projections of future capacity requirements shall be made to mitigate the risk of system overload.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization has allocated sufficient storage capacity to reduce the likelihood of exceeding capacity and the impact on network infrastructure (e.g., bandwidth).
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-04 (HIGH; MOD) ISO/IEC 27799:2016 12.1.3 MARS-E v2.2 - AU-4 NIST Cybersecurity Framework v1.1 - PR.DS-4 NY OHIP Moderate-Plus Security Baseline v5.0 - AU-4 NY OHIP Moderate-Plus Security Baseline v5.0 - AU-4[IS.1]

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 CMS Minimum Security Requirements (High) GDPR Supplemental
Level 2 Implementation (example):	The use of information and information system resources is monitored. Projections are made for future capacity requirements to ensure adequate systems performance. Capacity and monitoring procedures include the: identification of capacity requirements for each new and ongoing system/service; projection of future capacity requirements, considering current use, audit record storage requirements, projected trends, and anticipated changes in business requirements; and system monitoring and tuning to ensure and improve the availability and effectiveness of current systems.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.1 AICPA Trust Services Criteria - AICPA 2017 CC7.2 Banking Requirements - FFIEC IS v2016 A.8.1(p) CIS Controls v7.1 - CIS CSC v7.1 6.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-05 (HIGH; MOD) FedRAMP - SC-5[H] FedRAMP - SC-5[L] FedRAMP - SC-5[M] HIPAA Security Rule - § 164.312(b) ISO/IEC 27002:2022 - 8(6) ISO/IEC 27799:2016 12.1.3 NIST Cybersecurity Framework v1.1 - PR.DS-4 NIST SP 800-53 R4 SA-12(13)[S]{1} Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(e)
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization ensures that all systems that store logs have adequate storage space for the logs generated.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity. The information system provides an alert in real time to defined personnel, roles, and/or locations (defined in the applicable security plan) when the record log is full, upon authentication logging failure, and upon encryption logging failure.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system protects the availability of resources by allocating resources by priority or quota protection safeguards. The information system overwrites the oldest record in the event of an audit processing failure.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization allocates audit record storage capacity to retain audit records for the required audit retention period of seven years. The organization, in the event of an audit processing failure, monitors system operational status using operating system or system audit logs and verifies functions and performance of the system, or if logs are not available, shuts down the system.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity.

Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	The organization protects against or limits the effects of the types of denial-of-service attacks defined by NIST SP-800-61 R2, Computer Security Incident Handling Guide, the SANS Organization, the SANS Organization's Roadmap to Defeating DDoS, and the NIST CVE List National Vulnerability Database.

Control Reference: 09.i System Acceptance

Control Specification:	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance to maintain security.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. The organization ensures new information systems, upgrades, and new versions are only migrated into production after obtaining formal acceptance from management.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) ISO/IEC 27799:2016 14.2.2 ISO/IEC 27799:2016 14.2.9 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-10[PRIV.1a]

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	The organization requires the developer of the information system, system component, or information system service to: create and implement a security and privacy assessment plan; perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage; produce evidence of the execution of the security and privacy assessment plan and the results of the testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during testing/evaluation. The following action is carried out prior to formal acceptance being provided for a new system: an agreed set of security controls are in place; consultation with affected persons, or representatives of affected groups, at all phases of the process; preparation and testing of routine operating procedures to defined standards; effective manual procedures; evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end; evidence that an analysis has been carried out to the effect the new system has on the overall security of the organization; training in the operation or use of new systems; error recovery and restart procedures, and contingency plans; ease of use (as this affects user performance and avoids human error); and training in the new operation(s). The impact of the installation of any new system is thoroughly analyzed and tested with the coverage of the extreme operational conditions of the current systems.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.28(a) Banking Requirements - FFIEC IS v2016 A.6.28(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-11 (HIGH; MOD) FedRAMP - SA-11a[H] FedRAMP - SA-11a[M] FedRAMP - SA-11b[H] FedRAMP - SA-11b[M] FedRAMP - SA-11c[H] FedRAMP - SA-11c[M] FedRAMP - SA-11d[H] FedRAMP - SA-11d[M] FedRAMP - SA-11e[H] FedRAMP - SA-11e[M] Health Industry Cybersecurity Practices - 9.L.C HIPAA Security Rule - § 164.308(a)(4)(ii)(C) IRS Pub 1075 - SA-11a IRS Pub 1075 - SA-11b IRS Pub 1075 - SA-11c IRS Pub 1075 - SA-11d IRS Pub 1075 - SA-11e ISO/IEC 27799:2016 14.2.9 MARS-E v2.2 - SA-11a MARS-E v2.2 - SA-11b MARS-E v2.2 - SA-11c MARS-E v2.2 - SA-11d MARS-E v2.2 - SA-11e NIST Cybersecurity Framework v1.1 - DE.DP-3 NIST SP 800-53 R4 SA-11(7)[S]{0} NIST SP 800-53 R4 SA-11[HM]{0} NIST SP 800-53 R4 SA-15(1)[S]{1} NIST SP 800-53 R4 SA-4(3)[S]{0} NIST SP 800-53 R4 SA-4(5)a[S]{2} NIST SP 800-53 R4 SI-2b[HML]{0} NIST SP 800-53 r5 - SA-11 NIST SP 800-53 r5 - SA-11(7) NIST SP 800-53 r5 - SA-15(1)a NIST SP 800-53 r5 - SA-4(3)a NIST SP 800-53 r5 - SA-4(5)a NIST SP 800-53 r5 - SI-2b NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11[PRIV.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11a NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11b NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11c NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11d NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11e Supplemental Requirements - SR v6.4 29a.1-1 Supplemental Requirements - SR v6.4 30-0

Level CMS Implementation Requirements

Level CMS Implementation (example):	The organization requires the developer of the information system, system component, or information system service to: create and implement a security assessment plan in accordance with, but not limited to, current CMS procedures; perform unit; integration; system; regression testing/evaluation in accordance with the CMS system development life cycle governance process; produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during security testing/evaluation.

	The organization uses hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

Level FTI Custodians Implementation Requirements

Level HIX Implementation Requirements

Level HIX Implementation (example):	If the security control assessment results are used in support of the security authorization process for the information system, the organization ensures that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results.

Objective Name: 09.04 Protection Against Malicious and Mobile Code

Control Objective:	Ensure that integrity of information and software is protected from malicious or unauthorized code.

Control Reference: 09.j Controls Against Malicious Code

Control Specification:	Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	

Level 1 Regulatory Factors:	Community Supplemental Requirements 002 DirectTrust FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 1 Implementation (example):	Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution. The organization prohibits users from installing unauthorized software, including data and software from external networks, and disables any auto-run features which allow file execution without user authorization (such as when files are downloaded from the Internet or when removable media is inserted). Users are made aware and trained on requirements relating to prohibition of installing unauthorized software, including data and software from external networks.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.02(b)(2) 23 NYCRR 500 - 500.03(h) 23 NYCRR 500 - 500.05(a) AICPA Trust Services Criteria - AICPA 2017 CC6.8 Banking Requirements - FFIEC IS v2016 A.6.17 Banking Requirements - FFIEC IS v2016 A.8.1(a) CIS Controls v7.1 - CIS CSC v7.1 7.9 CIS Controls v7.1 - CIS CSC v7.1 8.1 CIS Controls v7.1 - CIS CSC v7.1 8.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-08(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-08(02) (HIGH; MOD) COBIT 5 DS5.9 COBIT 5 DSS05.01 Community Supplemental Requirements 002 - CSR002 v2018 7.1-1-0 Community Supplemental Requirements 002 - CSR002 v2018 7.1-2-0 Community Supplemental Requirements 002 - CSR002 v2018 7.1-3-0 Community Supplemental Requirements 002 - CSR002 v2018 7.1-4-0 FedRAMP - SI-2(3)a[H] FedRAMP - SI-3(2)[H] FedRAMP - SI-3(2)[M] FedRAMP - SI-3a[H] FedRAMP - SI-3a[L] FedRAMP - SI-3a[M] FedRAMP - SI-3b[H] FedRAMP - SI-3b[L] FedRAMP - SI-3b[M] FedRAMP - SI-8(1)[H] FedRAMP - SI-8(1)[M] FedRAMP - SI-8a[H] FedRAMP - SI-8a[M] FedRAMP - SI-8b[H] FedRAMP - SI-8b[M] Health Industry Cybersecurity Practices - 1.M.A Health Industry Cybersecurity Practices - 1.S.A Health Industry Cybersecurity Practices - 2.L.F Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.308(a)(5)(ii)(B) HITRUST De-ID Framework - De-ID Framework v1 Anti-malware: General IRS Pub 1075 - CM-6(IRS-1) IRS Pub 1075 - CM-7(IRS-1) IRS Pub 1075 - S3-b IRS Pub 1075 - SC-35 IRS Pub 1075 - SI-3a IRS Pub 1075 - SI-8a IRS Pub 1075 - SI-8b ISO/IEC 27002:2022 - 8(1) ISO/IEC 27002:2022 - 8(19) ISO/IEC 27002:2022 - 8(7) ISO/IEC 27799:2016 12.2.1

Level 1 Authoritative Source Mapping (Cont.):	ISO/IEC 27799:2016 12.6.2 MARS-E v2.2 - SC-7a MARS-E v2.2 - SI-3(1) MARS-E v2.2 - SI-3a MARS-E v2.2 - SI-3c MARS-E v2.2 - SI-3d1 MARS-E v2.2 - SI-8(1) MARS-E v2.2 - SI-8a MARS-E v2.2 - SI-8b NIST Cybersecurity Framework v1.1 - DE.CM-4 NIST Cybersecurity Framework v1.1 - DE.DP-5 NIST Cybersecurity Framework v1.1 - PR.DS-1 NIST Cybersecurity Framework v1.1 - RS.AN-1 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-171 r2 - 3.14.2[a] NIST SP 800-171 r2 - 3.14.2[b] NIST SP 800-171 r2 - 3.14.4[a] NIST SP 800-171 r2 - 3.14.5[a] NIST SP 800-171 r2 - 3.14.5[b] NIST SP 800-171 r2 - 3.14.5[c] NIST SP 800-53 R4 AC-4(5)[S]{1} NIST SP 800-53 R4 SC-25[S]{0} NIST SP 800-53 R4 SC-27[S]{0} NIST SP 800-53 R4 SC-29(1)[S]{0} NIST SP 800-53 R4 SC-30[S]{0} NIST SP 800-53 R4 SC-31(1)[S]{0} NIST SP 800-53 R4 SC-35[S]{0} NIST SP 800-53 R4 SI-3(4)[S]{0} NIST SP 800-53 R4 SI-3a[HML]{0} NIST SP 800-53 R4 SI-3b[HML]{0} NIST SP 800-53 R4 SI-3c[HML]{0} NIST SP 800-53 R4 SI-7(3)[S]{0} NIST SP 800-53 R4 SI-8(1)[HM]{0} NIST SP 800-53 R4 SI-8(3)[S]{0} NIST SP 800-53 R4 SI-8a[HM]{0} NIST SP 800-53 R4 SI-8b[HM]{0} NIST SP 800-53 r5 - AC-4(5) NIST SP 800-53 r5 - SC-25 NIST SP 800-53 r5 - SC-27 NIST SP 800-53 r5 - SC-29(1) NIST SP 800-53 r5 - SC-30 NIST SP 800-53 r5 - SC-31(1) NIST SP 800-53 r5 - SC-35 NIST SP 800-53 r5 - SI-3(4) NIST SP 800-53 r5 - SI-3a NIST SP 800-53 r5 - SI-3b NIST SP 800-53 r5 - SI-3c NIST SP 800-53 r5 - SI-7(3) NIST SP 800-53 r5 - SI-8(3) NIST SP 800-53 r5 - SI-8a NIST SP 800-53 r5 - SI-8b NY OHIP Moderate-Plus Security Baseline v5.0 - AC-17[IS.3d] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[IS.4a] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[IS.4b] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[IS.4c] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[PHI.4a] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[PHI.4b] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[PHI.4c] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-3a NY OHIP Moderate-Plus Security Baseline v5.0 - SI-3c1

Level 1 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - SI-3c2 NY OHIP Moderate-Plus Security Baseline v5.0 - SI-8[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-8[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-8a NY OHIP Moderate-Plus Security Baseline v5.0 - SI-8b PCI DSS v3.2.1 5.1 PCI DSS v3.2.1 5.1.1 PCI DSS v3.2.1 5.2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(7) Supplemental Requirements - SR v6.4 25a-0 Veterans Affairs Cybersecurity Program Directive 6500 - c92)(h)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Community Supplemental Requirements 002 FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	Anti-virus or anti-spy software (e.g., anti-malware) generates audit logs of checks performed. Protection against malicious code is based on malicious code detection and repair software, security awareness, appropriate system access, and change management controls.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.8 Banking Requirements - FFIEC IS v2016 A.6.17 CIS Controls v7.1 - CIS CSC v7.1 7.8 CIS Controls v7.1 - CIS CSC v7.1 8.1 CIS Controls v7.1 - CIS CSC v7.1 8.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03(01) (HIGH; MOD) COBIT 5 DS5.9 COBIT 5 DSS05.01 Community Supplemental Requirements 002 - CSR002 v2018 5.3-0-0 Community Supplemental Requirements 002 - CSR002 v2018 5.4-0-1 FedRAMP - SC-2[H] FedRAMP - SC-2[M] FedRAMP - SI-16[H] FedRAMP - SI-16[L] FedRAMP - SI-16[M] FedRAMP - SI-3(1)[H] FedRAMP - SI-3(1)[M] FedRAMP - SI-3c2[H] FedRAMP - SI-3c2[L] FedRAMP - SI-3c2[M] FedRAMP - SI-3d[H] FedRAMP - SI-3d[L] FedRAMP - SI-3d[M] Health Industry Cybersecurity Practices - 2.M.A HIPAA Security Rule - § 164.308(a)(5)(ii)(B) HITRUST De-ID Framework - De-ID Framework v1 Anti-malware: General IRS Pub 1075 - SC-2 IRS Pub 1075 - SI-16 IRS Pub 1075 - SI-3c2 IRS Pub 1075 - SI-3d ISO/IEC 27799:2016 12.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - SC-2 MARS-E v2.2 - SI-16 MARS-E v2.2 - SI-3e NIST Cybersecurity Framework v1.1 - DE.CM-4 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST SP 800-171 r2 - 3.13.3[a] NIST SP 800-171 r2 - 3.13.3[b] NIST SP 800-171 r2 - 3.13.3[c] NIST SP 800-53 R4 SC-2(1)[S]{0} NIST SP 800-53 R4 SC-2[HM]{0} NIST SP 800-53 R4 SC-29[S]{0} NIST SP 800-53 R4 SC-3(2)[S]{0} NIST SP 800-53 R4 SC-3(3)[S]{0} NIST SP 800-53 R4 SC-7(13)[S]{0} NIST SP 800-53 R4 SI-16[HM]{0} NIST SP 800-53 R4 SI-3(1)[HM]{0} NIST SP 800-53 R4 SI-3d[HML]{0} NIST SP 800-53 r5 - SC-2 NIST SP 800-53 r5 - SC-2(1) NIST SP 800-53 r5 - SC-2(2) NIST SP 800-53 r5 - SC-29 NIST SP 800-53 r5 - SC-3(2)

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - SC-3(3) NIST SP 800-53 r5 - SC-7(13) NIST SP 800-53 r5 - SI-16 NIST SP 800-53 r5 - SI-3d NY OHIP Moderate-Plus Security Baseline v5.0 - SC-2 NY OHIP Moderate-Plus Security Baseline v5.0 - SC-2[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-16 NY OHIP Moderate-Plus Security Baseline v5.0 - SI-16[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-3d PCI DSS v3.2.1 5.1.1 PCI DSS v3.2.1 5.1.2 PCI DSS v3.2.1 5.2 PCI DSS v3.2.1 5.3
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization enables anti-exploitation features, e.g., Data Execution Prevention (DEP), Windows Defender Exploit Guard (WDEG), Enhanced Mitigation Experience Toolkit (EMET), and Address Space Layout Randomization (ASLR), in its operating systems and applies anti-exploitation protections to a broader set of applications and executables by deploying additional capabilities, such as the Enhanced Migration Experience Toolkit. The anti-exploitation protection requirements are fully assessed by the organization prior to implementation due to potential difficulties (compatibility issues, etc.).
Level CMS Implementation Requirements	
Level CMS Implementation (example):	Desktop malicious code scanning software is configured to perform critical system file scans every 12 hours.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization implements non-signature based malicious code detection mechanisms to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code protection mechanisms are configured to perform periodic scans of the information system at least weekly and real-time scans of files from external sources to include endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization establishes policies governing the installation of software by users, enforces software installation policies through automated methods, and monitors software installation policy compliance on a continual basis. The organization implements malware protection at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	Desktop malicious code scanning software is configured to perform critical system file scans every 24 hours.
Level Community Supplemental Requirements 002 Implementation Requirements	

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization updates malicious code protection mechanisms whenever new releases are available in accordance with CMS configuration management policy and procedures. Malicious code scanning software on servers (to include databases and applications) is configured to perform critical system file scans no less often than once every 12 hours and full system scans no less often than once every 72 hours.

Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization uses an advanced protection technology to automatically remove email messages from the inbox of all users if a message is determined to be malicious after delivery. The organization implements endpoint detection and response (EDR) technologies on all endpoints for which such tools are available.

Control Reference: 09.k Controls Against Mobile Code

Control Specification:	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Community Supplemental Requirements 002
Level 1 Implementation (example):	The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.17 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03 (HIGH) Community Supplemental Requirements 002 - CSR002 v2018 5.4-0-2 Health Industry Cybersecurity Practices - 1.S.A Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.308(a)(5)(ii)(B) ISO/IEC 27799:2016 12.2.1 NIST Cybersecurity Framework v1.1 - DE.CM-4 NIST Cybersecurity Framework v1.1 - DE.CM-5 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-17[IS.3b]

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	Automated controls (e.g., browser settings) are in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations). The organization blocks any use and receipt (e.g., downloading and execution) of mobile code. The following actions are carried out to protect against mobile code performing unauthorized actions: a logically isolated environment is established for executing mobile code; technical measures are activated as available on a specific system to ensure mobile code performing unauthorized actions is managed; and resources with access to mobile code performing unauthorized actions is controlled.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC8.1 Banking Requirements - FFIEC IS v2016 A.6.17 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-02 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-03 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-18 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-18 (HIGH; MOD) IRS Pub 1075 - SC-18(1) ISO/IEC 27002:2022 - 8(4) ISO/IEC 27799:2016 12.2.1 ISO/IEC 27799:2016 12.5.1 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - DE.CM-5 NIST SP 800-171 r2 - 3.13.13[a] NIST SP 800-171 r2 - 3.13.13[b]

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization: defines acceptable and unacceptable mobile code and mobile code technologies; establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and authorizes, monitors, and controls the use of mobile code within the information system.

Objective Name: 09.05 Information Back-Up

Control Objective:	Ensure the maintenance, integrity, and availability of organizational information.

Control Reference: 09.l Back-up

Control Specification:	Back-up copies of information and software shall be taken and tested regularly.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust The Joint Commission v2016 PCI DSS v3.2.1 Texas Medical Records Privacy Act High Low Moderate Supplemental
Level 1 Implementation (example):	Backup copies of information and software are made regularly at appropriate intervals in accordance with an agreed-upon backup policy, are made when equipment is moved (relocated), and are tested regularly at appropriate intervals in accordance with an agreed-upon backup policy. Restoration procedures are tested regularly at appropriate intervals in accordance with an agreed-upon backup policy. A formal definition of the level of backup required for each system is defined and documented including the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory, and business requirements. The organization formally defines and documents how each system is completely restored from backup.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.06(a)(1) AICPA Trust Services Criteria - AICPA 2017 A1.2 CIS Controls v7.1 - CIS CSC v7.1 10.3 CIS Controls v7.1 - CIS CSC v7.1 10.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-04 (HIGH; MOD) FedRAMP - CP-6a[H] FedRAMP - CP-6a[M] FedRAMP - CP-6b[H] FedRAMP - CP-6b[M] Health Industry Cybersecurity Practices - 4.M.D Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.308(a)(7)(ii)(B) HIPAA Security Rule - § 164.310(d)(2)(iv) ISO/IEC 27002:2022 - 8(13) ISO/IEC 27799:2016 12.3.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - CP-6a MARS-E v2.2 - CP-6b NIST Cybersecurity Framework v1.1 - PR.IP-4 NIST SP 800-53 R4 CP-10(6)[S]{0} NIST SP 800-53 R4 CP-9[HML]{1} NIST SP 800-53 r5 - CP-10(6) NIST SP 800-53 r5 - CP-9 NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(1)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(1)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-9[PHI.1] OCR Audit Protocol (2016) 164.310(d)(2)(iv) PCI DSS v3.2.1 9.5.1 The Joint Commission (v2016) - TJC IM.01.01.03, EP 4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)? No

Level 2 Regulatory Factors:	The Joint Commission v2016 CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Texas Medical Records Privacy Act GDPR High Low Moderate
Level 2 Implementation (example):	Inventory records for the backup copies are maintained, include the content of the backup copies, and include the current location of the backup copies. When the backup service is delivered by the third-party, the service level agreement includes the detailed protections to control confidentiality, integrity, and availability of the backup information.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.2 CIS Controls v7.1 - CIS CSC v7.1 10.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-06(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-28 (HIGH; MOD) Health Industry Cybersecurity Practices - 4.M.D Health Industry Cybersecurity Practices - 4.S.B HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.310(d)(2)(iii) HIPAA Security Rule - § 164.310(d)(2)(iv) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(2)(ii) IRS Pub 1075 - CP-9(8) ISO/IEC 27799:2016 12.3.1 ISO/IEC 27799:2016 15.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - CP-9a NIST Cybersecurity Framework v1.1 - PR.IP-4 NIST SP 800-171 r2 - 3.8.9[a] NIST SP 800-53 R4 CP-9[HML]{2} NIST SP 800-53 r5 - CP-9 NIST SP 800-53 r5 - CP-9(8) NIST SP 800-53 r5 - SA-9(7) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-9(8) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-9[IS.2] PCI DSS v3.2.1 9.5.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records

Level 3 System Factors:	
Level 3 Regulatory Factors:	DirectTrust FedRAMP FISMA CMS Minimum Security Requirements (High) High Moderate
Level 3 Implementation (example):	The organization performs full backups weekly to separate media and incremental or differential backups daily to separate media. Three generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups are logged with name, date, time, and action.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(05) (HIGH) FedRAMP - CP-9(1)[M] FedRAMP - CP-9a[H] FedRAMP - CP-9a[L] FedRAMP - CP-9a[M] FedRAMP - CP-9b[H] FedRAMP - CP-9b[L] FedRAMP - CP-9b[M] HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.310(d)(2)(iv) IRS Pub 1075 - CP-9a IRS Pub 1075 - CP-9b ISO/IEC 27799:2016 12.3.1 NIST Cybersecurity Framework v1.1 - PR.IP-4 NIST SP 800-53 R4 CP-9(1)[HM]{0} NIST SP 800-53 r5 - CP-9(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-9[IS.1]
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization automatically backs up each system on a regular basis and ensures that each of the organization’s key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	Backups include copies of: user-level information; system-level information (including system state information); the operating system; other critical information system software; and the information system inventory (including hardware, software, and firmware components). The organization transfers information system backup information to the alternate storage site at defined time periods (defined in the applicable security plan) and transfer rates (defined in the applicable security plan) consistent with the recovery time and recovery point objectives.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The service provider determines what elements of the cloud environment require the Information System Backup control, how Information System Backup is going to be verified, and appropriate periodicity of the check. The service provider maintains at least three backup copies of user-level information, system-level information, and information system documentation (at least one of which is available online) or provides an equivalent alternative.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization protects the confidentiality of backup information at storage locations pursuant to IRC 6013. Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need-to-know.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization ensures a current, retrievable copy of personally identifiable information (PII) is available before the movement of servers. For cloud environments, the system owner determines what elements of the cloud environment require backups, how backups will be verified, and the appropriate periodicity of the check.
Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation (example):	The organization maintains backups of systems designed to reconstruct material financial transactions to support normal operations and obligations of the organization for five years.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization tests backup information following each backup, at least every six months for Moderate systems, to verify media reliability and information integrity.
Level HICP Implementation Requirements	

Objective Name: 09.06 Network Security Management

Control Objective:	Ensure the protection of information in networks and protection of the supporting network infrastructure.
Control Reference: 09.m Network Controls	
Control Specification:	Networks shall be managed and controlled in order to protect the organization from threats and to maintain security for the systems and applications using the network, including information in transit.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	Are wireless access points in place at any of the organization's in-scope facilities? No
Level 1 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) GDPR Supplemental
Level 1 Implementation (example):	Prior to authorizing the implementation of wireless access points, the organization changes vendor default encryption keys, default SNMP community strings on wireless devices, default passwords/passphrases on access points, and other security-related wireless vendor defaults, if applicable. The organization changes wireless encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.10 Banking Requirements - FFIEC IS v2016 A.6.7(b) Banking Requirements - FFIEC IS v2016 A.6.7(c) Banking Requirements - FFIEC IS v2016 A.8.1(a) Banking Requirements - FFIEC IS v2016 A.8.1(h) Banking Requirements - FFIEC IS v2016 A.8.4 CIS Controls v7.1 - CIS CSC v7.1 12.3 CIS Controls v7.1 - CIS CSC v7.1 12.6 CIS Controls v7.1 - CIS CSC v7.1 12.7 CIS Controls v7.1 - CIS CSC v7.1 13.4 CIS Controls v7.1 - CIS CSC v7.1 15.1 CIS Controls v7.1 - CIS CSC v7.1 15.5 CIS Controls v7.1 - CIS CSC v7.1 15.6 CIS Controls v7.1 - CIS CSC v7.1 15.7 CIS Controls v7.1 - CIS CSC v7.1 9.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DSS05.02 Community Supplemental Requirements 002 - CSR002 v2018 11.2-1-1 Community Supplemental Requirements 002 - CSR002 v2018 4.2-2-0 Health Industry Cybersecurity Practices - 2.L.C Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 6.M.C Health Industry Cybersecurity Practices - 6.M.D Health Industry Cybersecurity Practices - 6.M.E Health Industry Cybersecurity Practices - 6.S.A Health Industry Cybersecurity Practices - 6.S.C Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.308(a)(1)(ii)(B) IRS Pub 1075 - 3.3.6(3) IRS Pub 1075 - 3.3.6(5) IRS Pub 1075 - SC-7(5) ISO/IEC 27002:2022 - 8(23) ISO/IEC 27799:2016 13.1.1 ISO/IEC 27799:2016 13.1.3 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - SC-7(12) MARS-E v2.2 - SI-4a1 NIST Cybersecurity Framework v1.1 - DE.AE-1 NIST Cybersecurity Framework v1.1 - DE.AE-3 NIST Cybersecurity Framework v1.1 - DE.CM-1 NIST Cybersecurity Framework v1.1 - DE.DP-5 NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-171 r2 - 3.1.16[b] NIST SP 800-171 r2 - 3.1.17[b] NIST SP 800-53 R4 CA-3a[HML]{0} NIST SP 800-53 R4 CA-9[HML]{0} NIST SP 800-53 R4 CM-7a[HML]{3} NIST SP 800-53 R4 SC-40(2)[S]{0} NIST SP 800-53 R4 SC-41[S]{0}

Level 1 Authoritative Source Mapping (Cont.):	NIST SP 800-53 R4 SI-4(15)[S]{0} NIST SP 800-53 r5 - CA-3(6) NIST SP 800-53 r5 - CA-3(7)a NIST SP 800-53 r5 - CA-3a NIST SP 800-53 r5 - CM-7a NIST SP 800-53 r5 - RA-10 NIST SP 800-53 r5 - SA-8(23) NIST SP 800-53 r5 - SC-40(2) NIST SP 800-53 r5 - SC-5b NIST SP 800-53 r5 - SI-4(15) NIST SP 800-53 r5 - SI-4(25) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1f] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)[IS.1h] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)f NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7(4)h NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4[PHI.1a] PCI DSS v3.2.1 1.2.3 PCI DSS v3.2.1 11.4 PCI DSS v3.2.1 2.1.1 PCI DSS v3.2.1 4.1.1 Supplemental Requirements - SR v6.4 4-0 Supplemental Requirements - SR v6.4 42.2-0 Supplemental Requirements - SR v6.4 45a-1
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	Community Supplemental Requirements 002 DirectTrust FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) GDPR High Low Moderate Supplemental
Level 2 Implementation (example):	A current network diagram exists, documents all high-risk environments, documents all data flows, documents all connections to systems storing, processing, or transmitting covered information, and documents any wireless networks that may have legal compliance impacts. The network diagram is updated based on changes to the network and no less than every six months. The organization monitors for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAP) unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.10 Banking Requirements - FFIEC IS v2016 A.6.18(d) Banking Requirements - FFIEC IS v2016 A.6.7(a) Banking Requirements - FFIEC IS v2016 A.6.7(b) Banking Requirements - FFIEC IS v2016 A.6.7(c) CIS Controls v7.1 - CIS CSC v7.1 11.1 CIS Controls v7.1 - CIS CSC v7.1 11.2 CIS Controls v7.1 - CIS CSC v7.1 11.3 CIS Controls v7.1 - CIS CSC v7.1 12.3 CIS Controls v7.1 - CIS CSC v7.1 13.4 CIS Controls v7.1 - CIS CSC v7.1 15.2 CIS Controls v7.1 - CIS CSC v7.1 15.8 CIS Controls v7.1 - CIS CSC v7.1 9.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08 (HIGH; MOS) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-19 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DSS05.02 Community Supplemental Requirements 002 - CSR002 v2018 11.1-0-0 Community Supplemental Requirements 002 - CSR002 v2018 11.1-0-1 Community Supplemental Requirements 002 - CSR002 v2018 11.1-0-3 Community Supplemental Requirements 002 - CSR002 v2018 11.2-1-1 Community Supplemental Requirements 002 - CSR002 v2018 11.2-1-2 Community Supplemental Requirements 002 - CSR002 v2018 11.3-0-1 Community Supplemental Requirements 002 - CSR002 v2018 4.2-1-0 Community Supplemental Requirements 002 - CSR002 v2018 4.2-2-0 FedRAMP - CA-3(5)[H] FedRAMP - CA-3(5)[M] FedRAMP - CA-3a[H] FedRAMP - CA-3a[L] FedRAMP - CA-3a[M] FedRAMP - CA-3b[H] FedRAMP - CA-3b[L] FedRAMP - CA-3b[M] FedRAMP - SC-19a[H] FedRAMP - SC-19a[M] FedRAMP - SC-19b[H] FedRAMP - SC-19b[M] FedRAMP - SC-7(4)c[H] FedRAMP - SC-7(4)c[M] FedRAMP - SC-8[H] FedRAMP - SC-8[M] Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 6.M.A HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(iii) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(e)(1)

Level 2 Authoritative Source Mapping (Cont.):	HIPAA Security Rule - § 164.312(e)(2)(i) HIPAA Security Rule - § 164.312(e)(2)(ii) HITRUST De-ID Framework - De-ID Framework v1 Transmission Encryption: Policies IRS Pub 1075 - CA-3a IRS Pub 1075 - CA-3b IRS Pub 1075 - SC-7(4)c IRS Pub 1075 - SC-8 ISO/IEC 27002:2022 - 8(20) ISO/IEC 27799:2016 13.1.1 ISO/IEC 27799:2016 13.1.2 ISO/IEC 27799:2016 13.1.3 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-18a MARS-E v2.2 - CA-3(5) MARS-E v2.2 - CA-3a MARS-E v2.2 - CA-3b MARS-E v2.2 - MP-5e MARS-E v2.2 - SC-19a MARS-E v2.2 - SC-19b MARS-E v2.2 - SC-8(1) MARS-E v2.2 - SC-8(2) NIST Cybersecurity Framework v1.1 - ID.AM-3 NIST Cybersecurity Framework v1.1 - PR.DS-4 NIST Cybersecurity Framework v1.1 - PR.IP-3 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST Cybersecurity Framework v1.1 - RS.AN-2 NIST SP 800-171 r2 - 3.1.3[a] NIST SP 800-171 r2 - 3.1.3[b] NIST SP 800-171 r2 - 3.1.3[c] NIST SP 800-171 r2 - 3.1.3[d] NIST SP 800-171 r2 - 3.1.3[e] NIST SP 800-171 r2 - 3.13.14[a] NIST SP 800-171 r2 - 3.13.14[b] NIST SP 800-171 r2 - 3.13.8[a] NIST SP 800-171 r2 - 3.13.8[b] NIST SP 800-171 r2 - 3.13.8[c] NIST SP 800-53 R4 AC-18(1)[HM]{1} NIST SP 800-53 R4 CA-3a[HML]{0} NIST SP 800-53 R4 CA-9(1)[S]{0} NIST SP 800-53 R4 CA-9[HML]{0} NIST SP 800-53 R4 IA-5(6)[S]{0} NIST SP 800-53 R4 IA-9(2)[S]{0} NIST SP 800-53 R4 SA-4(6)a[S]{1} NIST SP 800-53 R4 SA-4(7)b[S]{0} NIST SP 800-53 R4 SC-16(1)[S]{0} NIST SP 800-53 R4 SC-19[HM]{0} NIST SP 800-53 R4 SC-28(1)[S]{0} NIST SP 800-53 R4 SC-40(4)[S]{0} NIST SP 800-53 R4 SC-7(4)c[HM]{0} NIST SP 800-53 R4 SC-8(1)[HM]{0} NIST SP 800-53 R4 SC-8(2)[S]{0} NIST SP 800-53 R4 SC-8(3)[S]{0} NIST SP 800-53 R4 SC-8[HM]{0} NIST SP 800-53 r5 - AC-18(1) NIST SP 800-53 r5 - CA-3(6) NIST SP 800-53 r5 - CA-3(7)a NIST SP 800-53 r5 - CA-3a NIST SP 800-53 r5 - CA-9(1) NIST SP 800-53 r5 - IA-3 NIST SP 800-53 r5 - IA-5(6)

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - SA-4(6)a NIST SP 800-53 r5 - SA-4(7)b NIST SP 800-53 r5 - SA-8(23) NIST SP 800-53 r5 - SC-16(1) NIST SP 800-53 r5 - SC-40(4) NIST SP 800-53 r5 - SC-7(25) NIST SP 800-53 r5 - SC-7(4)c NIST SP 800-53 r5 - SC-7(4)f NIST SP 800-53 r5 - SC-8 NIST SP 800-53 r5 - SC-8(1) NIST SP 800-53 r5 - SC-8(2) NIST SP 800-53 r5 - SC-8(3) NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4(6) NY OHIP Moderate-Plus Security Baseline v5.0 - MA-4(6)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-8(1) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-8(1)[IS.1] PCI DSS v3.2.1 1.1 PCI DSS v3.2.1 1.1.1 PCI DSS v3.2.1 1.1.2 PCI DSS v3.2.1 1.1.3 PCI DSS v3.2.1 1.1.4 PCI DSS v3.2.1 1.2 PCI DSS v3.2.1 1.2.2 PCI DSS v3.2.1 1.3.3 PCI DSS v3.2.1 11.1 Supplemental Requirements - SR v6.4 10.4-0 Supplemental Requirements - SR v6.4 11-0 Supplemental Requirements - SR v6.4 42.2-0 Supplemental Requirements - SR v6.4 45a-1
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	Are wireless access points in place at any of the organization's in-scope facilities? No
Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High) High Moderate
Level 3 Implementation (example):	The impact of the loss of network service to the business is defined.

	The organization ensures firewall configuration standards and router configuration standards are defined. Firewall and router configuration standards address all connections to covered information, including any wireless networks. All connections to covered information, including any wireless networks, are supported by documented business justifications for the use of all services, protocols, and ports allowed. Firewall and router configuration standards include documentation of security features implemented for those protocols considered to be insecure. Firewall and router rule sets are reviewed and updated every 180 days.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 1.7 CIS Controls v7.1 - CIS CSC v7.1 11.1 CIS Controls v7.1 - CIS CSC v7.1 12.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-18(05) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-07(18) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-22 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-7(18) (HIGH) COBIT 5 DS5.10 COBIT 5 DSS05.02 Health Industry Cybersecurity Practices - 6.M.A Health Industry Cybersecurity Practices - 6.M.B ISO/IEC 27799:2016 13.1.1 ISO/IEC 27799:2016 13.1.3 MARS-E v2.2 - SC-7a NIST Cybersecurity Framework v1.1 - ID.RA-4 NIST SP 800-53 R4 SC-7(3)[HM]{0} NIST SP 800-53 r5 - PL-8(2) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[PHI.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-7[PHI.2] PCI DSS v3.2.1 1.1.4 PCI DSS v3.2.1 1.1.6 PCI DSS v3.2.1 1.1.7 PCI DSS v3.2.1 1.2.2 PCI DSS v3.2.1 1.3 PCI DSS v3.2.1 1.3.1 PCI DSS v3.2.1 1.3.2 PCI DSS v3.2.1 1.3.3 PCI DSS v3.2.1 1.3.4 PCI DSS v3.2.1 1.3.5 PCI DSS v3.2.1 1.3.6 PCI DSS v3.2.1 1.3.7 PCI DSS v3.2.1 1.3.8 PCI DSS v3.2.1 9.1.3 Supplemental Requirements - SR v6.4 10.3-0

Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization maintains and enforces network-based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization specifically blocks access to known file transfer and email exfiltration websites. The organization subscribes to URL categorization services to ensure that they are up to date with the most recent website category definitions available. Uncategorized are blocked by default. This filtering is enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. The organization enables DNS query logging to detect hostname lookup for known malicious command and control domains.

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Level Federal Implementation Requirements	

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system provides additional data origin integrity artifacts (e.g., digital signatures, cryptographic keys) along with authoritative data (e.g., DNS resource records) in response queries to obtain origin authentication and integrity verification assurances and the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources (e.g., by using a resolving or caching domain name system (DNS) server and authoritative DNS servers).

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization identifies and analyzes how FTI in a data warehouse is used and how FTI is queried or targeted by end users. Parts of the system containing FTI are mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. For a VoIP network that provides FTI to a customer, VoIP phones are logically protected and the VoIP traffic is encrypted using a NIST-approved method, operating in a NIST-approved mode, when FTI is in transit across the network (either Internet or state agency's network).

Level HIX Implementation Requirements	

Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization ensures network diagrams identify all cardholder data connections and data flows.

	The organization uses intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network, monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization protects workstations from potentially compromised peers by blocking inbound communication from other workstations and allowing only communication from administrative services. The organization utilizes a hardened intermediary system, running only a pre-defined set of applications (without Internet access or office productivity applications), to prevent end-users from directly communicating to administrative network zones and control privileged access for administrators, developers, and others who need greater network access than regular end-users, to perform their job duties.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	Firewalls from two or more different vendors are utilized at the various levels within the network to reduce the possibility of compromising the entire network. The information system protects the confidentiality and integrity of information and any transmitted data containing sensitive information is encrypted using a FIPS 140-2 validated module (see HHS Standard for Encryption of Computing Devices and Information).
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization employs advanced analytics (e.g., sandboxing) to test untrusted code and/or programs traversing through the network or system boundaries, in order to detect and block malicious content. The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization restricts the “send all” function of email distribution lists to authorized individuals. The organization ensures the following basic endpoint protections are implemented: enable full-disk encryption on all endpoints; disable weak authentication hashes on endpoints; and restrict local administrative rights on endpoints to authorized individuals.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The organization requires that providers of external system services comply with organizational security and privacy requirements and employ organization-defined controls commensurate with the protection mechanisms implemented by the external service provider, define and document organizational oversight and user roles and responsibilities with regard to external system services, and employ organization-defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis.

Control Reference: 09.n Security of Network Services

Control Specification:	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored. The right to audit is agreed by management for each network service provider. The security arrangements necessary for particular network services' security features, service levels, and management requirements, are identified and documented.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) Health Industry Cybersecurity Practices - 6.S.A ISO/IEC 27002:2022 - 8(21) ISO/IEC 27799:2016 13.1.2 NIST Cybersecurity Framework v1.1 - DE.CM-6 NIST Cybersecurity Framework v1.1 - ID.SC-1

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate

Level 2 Implementation (example):	The organization formally authorizes connections through the use of an interconnection security or other formal agreement. The organization centrally documents the interface characteristics of each connection, the security requirements of each connection, and the information communicated for each connection. The organization authorizes connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreements that: require providers to comply with organizational information security requirements; employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; define and document organizational oversight and user roles and responsibilities with regard to external information system services; provide for organizational monitoring of security control compliance by external service providers; require the use of FIPS-validated cryptographic mechanisms during transmission to protect the confidentiality and integrity of information unless otherwise protected by alternative physical measures; and state the provider is responsible for the protection of covered information.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.30 Banking Requirements - FFIEC IS v2016 A.6.7(a) Banking Requirements - FFIEC IS v2016 A.6.7(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-03(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09(02) (HIGH; MOD) FedRAMP - SA-9(2)[H] FedRAMP - SA-9(2)[M] HIPAA Privacy Rule - 164.504(e)(2)(ii)(D) HIPAA Security Rule - § 164.308(b)(1) HIPAA Security Rule - § 164.314(a)(1) HIPAA Security Rule - § 164.314(a)(2)(i)(A) HIPAA Security Rule - § 164.314(a)(2)(i)(B) HIPAA Security Rule - § 164.314(a)(2)(i)(C) IRS Pub 1075 - SA-9(2) ISO/IEC 27002:2022 - 5(15) MARS-E v2.2 - SA-9(2) NIST Cybersecurity Framework v1.1 - DE.AE-1 NIST Cybersecurity Framework v1.1 - DE.CM-6 NIST Cybersecurity Framework v1.1 - ID.AM-3 NIST Cybersecurity Framework v1.1 - ID.SC-1 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST SP 800-53 R4 CA-3b[HML]{0} NIST SP 800-53 R4 CA-3c[HML]{0} NIST SP 800-53 R4 SA-9(2)[HM]{0} NIST SP 800-53 R4 SA-9[HML]{0} NIST SP 800-53 r5 - CA-3b NIST SP 800-53 r5 - CA-3c NIST SP 800-53 r5 - CA-9d NIST SP 800-53 r5 - SA-9 NIST SP 800-53 r5 - SA-9(2) NY OHIP Moderate-Plus Security Baseline v5.0 - CA-3a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-17a
Level Cloud Service Providers Implementation Requirements	
Level Cloud Service Providers Implementation (example):	Business-critical or customer (tenant) impacting (physical and virtual) application and interface designs (API), configurations, network infrastructure, and systems components, are designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization records each system interconnection in the security plan for the system that is connected to the remote location. The Interconnection Security Agreement or data sharing agreement is updated following significant changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity of the agreement.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization requires external/outsourced service providers of all external systems where Federal information is processed or stored to identify the specific functions, ports, and protocols used in the provision of the external/outsourced services. The organization prohibits the direct connection of any system processing, transmitting, or storing Controlled Unclassified Information (CUI) to an external network without the use of a boundary protection device that meets Trusted Internet Connection (TIC) requirements.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization reviews and updates the system interconnection agreements on an annual basis.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization records each system interconnection in the security plan for the system that is connected to the remote location, and updates each interconnection security agreement following significant changes to the system, organization, or the nature of the electronic sharing of information that could impact the validity of the agreement. The organization establishes system-to-system connections with CMS through the Fed2NonFed Interconnection Security Agreement (ISA) process.

Objective Name: 09.07 Media Handling

Control Objective:	Prevent unauthorized disclosure, modification, removal or destruction of information assets, or interruptions to business activities.
Control Reference: 09.o Management of Removable Media	
Control Specification:	Formal procedures shall be documented and implemented for the management of removable media.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography, tamper-evident packaging, a securable container (e.g., locked briefcase) via authorized personnel if hand-carried, and a trackable receipt by commercial carrier if shipped. The organization: maintains accountability for information system media during transport outside of controlled areas; documents activities associated with the transport of information system media; and restricts the activities associated with transport of such media to authorized personnel. The organization restricts the use of writable, removable media and personally owned, removable media in organizational systems.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 13.7 CIS Controls v7.1 - CIS CSC v7.1 8.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05(04) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-07(01) (HIGH; MOD) FedRAMP - MP-6(3)[H] FedRAMP - MP-7[H] FedRAMP - MP-7[L] FedRAMP - MP-7[M] Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(iii) IRS Pub 1075 - MP-5(3) IRS Pub 1075 - MP-5a IRS Pub 1075 - MP-5b IRS Pub 1075 - MP-5c IRS Pub 1075 - MP-5d IRS Pub 1075 - MP-7(IRS-1)a IRS Pub 1075 - MP-7(IRS-1)b ISO/IEC 27799:2016 8.3.1 MARS-E v2.2 - MP-2a MARS-E v2.2 - MP-2b MARS-E v2.2 - MP-5a1 MARS-E v2.2 - MP-5a2 MARS-E v2.2 - MP-5b MARS-E v2.2 - MP-5c MARS-E v2.2 - MP-5d MARS-E v2.2 - MP-7a NIST Cybersecurity Framework v1.1 - PR.PT-2 NIST SP 800-171 r2 - 3.8.5[a] NIST SP 800-171 r2 - 3.8.5[b] NIST SP 800-171 r2 - 3.8.6[a] NIST SP 800-171 r2 - 3.8.7[a] NIST SP 800-171 r2 - 3.8.8[a] NIST SP 800-53 R4 MP-2[HML]{0} NIST SP 800-53 R4 MP-6(3)[H]{0} NIST SP 800-53 R4 MP-7[HML]{0} NIST SP 800-53 r5 - MP-2 NIST SP 800-53 r5 - MP-6(3) NIST SP 800-53 r5 - MP-7a NY OHIP Moderate-Plus Security Baseline v5.0 - MP-2[IS.3a] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-2[IS.3b] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-7[PRIV.1] NY OHIP Moderate-Plus Security Baseline v5.0 - MP-7a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-7(1)[IS.1b] PCI DSS v3.2.1 9.6.3 Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(c)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act Supplemental
Level 2 Implementation (example):	The organization formally establishes and enforces controls (e.g., policies and procedures) for the management of removable media and laptops including: restrictions on the type(s) of media, and usages thereof to maintain security; and registration of certain type(s) of media and laptops. Media containing covered and/or confidential information is physically stored and its data encrypted in accordance with the organization's data protection and privacy policy on the use of cryptographic controls until the media are destroyed or sanitized and commensurate with the confidentiality and integrity requirements for its data classification level. The organization identifies digital media requiring restricted use, non-digital media requiring restricted use, and the specific safeguards necessary to restrict use of digital and non-digital media requiring restricted use.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.21(d) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-07 (HIGH; MOD) FedRAMP - MP-2[H] FedRAMP - MP-2[L] FedRAMP - MP-2[M] Health Industry Cybersecurity Practices - 2.M.A HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.312(e)(2)(ii) IRS Pub 1075 - MP-2 ISO/IEC 27799:2016 8.3.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - MP-4a MARS-E v2.2 - MP-4b NIST Cybersecurity Framework v1.1 - PR.IP-6 NIST SP 800-171 r2 - 3.8.2[a] NIST SP 800-53 R4 MP-8[S]{1} NIST SP 800-53 R4 SA-12(9)[S]{1} NIST SP 800-53 r5 - MP-4 NIST SP 800-53 r5 - MP-6 NIST SP 800-53 r5 - MP-8 NIST SP 800-53 r5 - PE-22 NIST SP 800-53 r5 - SR-7 NY OHIP Moderate-Plus Security Baseline v5.0 - MP-4[PRIV.1] OCR Guidance for Unsecured PHI (1)(i) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(c) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(5) Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(c)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Authoritative Source Mapping:	

Level CIS Implementation Requirements

Level CMS Implementation Requirements

Level CMS Implementation (example):	The organization physically controls and securely stores digital media and non-digital media within controlled areas using physical security safeguards prescribed for the highest system security level of the information ever recorded on it, as defined within NIST SP 800-88, Guidelines for Media Sanitization.

	The organization evaluates employing an approved method of cryptography to protect PII at rest, consistent with NIST SP 800-66 guidance. If PII is recorded on magnetic media with other data, it is protected as if it were entirely personally identifiable information.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Media provided by visitors is only loaded into a standalone information system. The information system remains standalone until such time as it is sanitized. Other media loaded into the standalone information system is not loaded into a non-standalone information system until sanitized.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Control Reference: 09.p Disposal of Media

Control Specification:	Media shall be disposed of securely and safely when no longer required, using formal procedures that are documented.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust The Joint Commission v2016 PCI DSS v3.2.1 Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization destroys (e.g., disk wiping, degaussing, shredding, disintegration, grinding, incineration, pulverization or melting) media containing sensitive information when it is no longer needed for business or legal reasons.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.18(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06 (HIGH; MOD) Health Industry Cybersecurity Practices - 5.M.D Health Industry Cybersecurity Practices - 5.S.C Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(i) ISO/IEC 27002:2022 - 7(10) ISO/IEC 27002:2022 - 8(10) ISO/IEC 27799:2016 8.3.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - DM-2b MARS-E v2.2 - DM-2c NY OHIP Moderate-Plus Security Baseline v5.0 - SR-12 NY OHIP Moderate-Plus Security Baseline v5.0 - SR-12[IS.1] OCR Guidance for Unsecured PHI (2)(i) OCR Guidance for Unsecured PHI (2)(ii) PCI DSS v3.2.1 9.8 The Joint Commission (v2016) - TJC IM.02.01.03, EP 3
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FISMA The Joint Commission v2016 PCI DSS v3.2.1 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Formal procedures for the secure disposal of media minimizes the risk of information leakage to unauthorized persons. If collection and disposal services offered by other organizations are used, care is taken in selecting a suitable contractor with adequate controls and experience.

	Media is disposed in a manner commensurate with the sensitivity of the information contained on the media using generally accepted and secure disposal or erasure methods for media that contains (or might contain) covered and/or confidential information. Procedures for the secure disposal of media containing information address the identification of information that qualifies as covered (otherwise a policy is developed that all information is considered covered in the absence of unequivocal evidence to the contrary).
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.5 Banking Requirements - FFIEC IS v2016 A.6.18(e) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-06(02) (HIGH) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(i) HIPAA Security Rule - § 164.310(d)(2)(ii) IRS Pub 1075 - PL-2(IRS-1) ISO/IEC 27799:2016 8.3.2 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.DS-5 NIST SP 800-53 R4 MP-8[S]{2} NIST SP 800-53 r5 - MP-8 OCR Guidance for Unsecured PHI (2)(i) OCR Guidance for Unsecured PHI (2)(ii) Ontario Personal Health Information Protection Act - 13(1) Supplemental Requirements - SR v6.4 17.7-0 The Joint Commission (v2016) - TJC IM.02.01.03, EP 3 Veterans Affairs Cybersecurity Program Directive 6500 - a(2)(c)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization reviews, approves, tracks, documents (logs), and verifies media sanitization and disposal actions. The organization tests sanitization equipment and procedures within every 365 days to verify that the intended sanitization is being achieved.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization tests sanitization equipment and procedures within every 365 days to verify that the intended sanitization is being achieved. The organization tests sanitization equipment and procedures within every six months to verify that the intended sanitization is being achieved.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization: cleanses FTI at the staging area of a data warehouse; documents how it cleanses the FTI when it is extracted, transformed, and loaded (i.e., in the ETL process); describes the process of object reuse once FTI is replaced from data sets. All FTI must be removed from media in the data warehouse by a random overwrite software program. Media sanitization requirements are established as applicable for media used in pre-production or test environments: the technique for clearing, purging, and destroying media are the same, regardless of where the information system media is located; every third piece of media must be tested after sanitization has been completed; and media sanitization is witnessed or verified by the organization’s employee.

Level HIX Implementation Requirements	

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization finely shreds, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Control Reference: 09.q Information Handling Procedures

Control Specification:	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	State of Massachusetts Data Protection Act (201 CMR 17.00) High Moderate Supplemental
Level 1 Implementation (example):	Media is labeled, encrypted, and handled according to its classification.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(ii) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-03 (HIGH; MOD) Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(2)(ii) IRS Pub 1075 - 2.B.4(1) IRS Pub 1075 - 2.C.5.1(2)b ISO/IEC 27002:2022 - 7(10) ISO/IEC 27799:2016 8.2.3 MARS-E v2.2 - MP-3a MARS-E v2.2 - MP-5a1 NIST SP 800-53 R4 AC-16b[S]{2} NIST SP 800-53 R4 MP-3[HM]{0} NIST SP 800-53 r5 - AC-16b NIST SP 800-53 r5 - MP-3 PCI DSS v3.2.1 9.5 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(c) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(g)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00)
Level 2 Implementation (example):	The status and location of unencrypted covered and/or confidential information is maintained and monitored. The organization maintains inventories of media to manage strict controls over storage and accessibility. Management approves any and all media that is moved from a secured area, especially when media is distributed to individuals. Formal records of data transfers, including logging and an audit trail, are maintained.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(ii) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-12 (HIGH; MOD) ISO/IEC 27799:2016 8.2.3 Legacy Inheritance Support - L.I.S. PCI DSS v3.2.1 3.2 PCI DSS v3.2.1 3.2.1 PCI DSS v3.2.1 3.2.2 PCI DSS v3.2.1 3.2.3 PCI DSS v3.2.1 9.6 PCI DSS v3.2.1 9.6.3 PCI DSS v3.2.1 9.7
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	

Level 3 Regulatory Factors:	FedRAMP CMS Minimum Security Requirements (High) High Moderate
Level 3 Implementation (example):	Inventory and disposition records for information system media are maintained to ensure control and accountability of the organization's information. Inventory and disposition of media-related records contain sufficient information to reconstruct the data in the event of a breach, including, at a minimum: the name of media recipient; the signature of media recipient; the date/time media is received; the media control number and contents; the movement or routing information; and if disposed of, the date, time, and method of destruction. The organization implements cryptographic mechanisms to protect the confidentiality and integrity of sensitive (non-public) information stored on digital media during transport outside of controlled areas.
Level 3 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05(04) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-CMS-1 (HIGH; MOD) FedRAMP - MP-5(4)[H] FedRAMP - MP-5(4)[M] Health Industry Cybersecurity Practices - 5.S.A HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.310(d)(2)(iii) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(e)(2)(i) HIPAA Security Rule - § 164.312(e)(2)(ii) MARS-E v2.2 - MP-5(4) MARS-E v2.2 - MP-CMS-1 NIST SP 800-53 R4 MP-5(4)[HM]{0} NIST SP 800-53 r5 - SA-9(6)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization conducts semi-annual inventories of removable media containing PII.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization marks all information system media, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. The organization protects and controls all media with sensitive information during transport outside of controlled areas prior to leaving the secure/controlled environment including for digital media, with encryption using a FIPS 140-2 validated encryption module, and for non-digital media, secured in locked container. The organization maintains accountability for information system media during transport outside of controlled areas, documents activities associated with the transport of information system media, and restricts the activities associated with the transport of information system media to authorized personnel.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization employs automated mechanisms to: restrict access to sensitive information (e.g., PII) residing on digital media to authorized individuals; restrict access to sensitive information (e.g., PII) residing on non-digital media to authorized individuals; restrict access to media storage areas; audit access attempts to media storage areas; and audit access granted to media storage areas.

	Inventory and disposition records for information system media are maintained to ensure control and accountability of CMS information. Further, ensure the media-related records contain sufficient information to reconstruct the data in the event of a breach.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The system does not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, the system renders all data unrecoverable upon completion of the authorization process. The system does not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. The system does not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization. The system does not store the personal identification number (PIN) or the encrypted PIN block after authorization.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	Commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data, the organization: protects and controls digital and non-digital media defined within the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS Information Systems Security and Privacy Policy (IS2P) Appendix I, containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging, and: if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel; or if shipped, trackable with receipt by commercial carrier; maintains accountability for information system media during transport outside of controlled areas; documents activities associated with the transport of information system media; and restricts the activities associated with the transport of information system media to authorized personnel. The organization defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the Joint Authorization Board (JAB).

Control Reference: 09.r Security of System Documentation

Control Specification:	System documentation shall be protected against unauthorized access.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The access list for system documentation is kept to a minimum and is authorized by the application owner.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-05 (HIGH; MOD)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	The organization obtains administrator documentation for the information system, system component, or information system service that describes: secure configuration, installation, and operation of the system, component, or service; effective use and maintenance of security and privacy functions/mechanisms; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. The organization obtains user documentation for the information system, system component, or information system service that describes: user-accessible security and privacy functions/mechanisms and how to effectively use those functions/mechanisms; methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and user responsibilities in maintaining the security and privacy of the system, component, or service. Organizations document attempts to obtain information system documentation when such documentation is either unavailable or non-existent. The organization protects system documentation in accordance with the organization's risk management strategy and distributes documentation to organization-defined personnel with the need for such documentation.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-05 (HIGH; MOD) FedRAMP - SA-5a1[H] FedRAMP - SA-5a1[L] FedRAMP - SA-5a1[M] FedRAMP - SA-5a2[H] FedRAMP - SA-5a2[L] FedRAMP - SA-5a2[M] FedRAMP - SA-5a3[H] FedRAMP - SA-5a3[L] FedRAMP - SA-5a3[M] FedRAMP - SA-5b1[H] FedRAMP - SA-5b1[L] FedRAMP - SA-5b1[M] FedRAMP - SA-5b2[H] FedRAMP - SA-5b2[L] FedRAMP - SA-5b2[M] FedRAMP - SA-5b3[H] FedRAMP - SA-5b3[L] FedRAMP - SA-5b3[M] HIPAA Security Rule - § 164.316(b)(2)(ii) IRS Pub 1075 - SA-5a1 IRS Pub 1075 - SA-5a2 IRS Pub 1075 - SA-5a3 IRS Pub 1075 - SA-5b1 IRS Pub 1075 - SA-5b2 IRS Pub 1075 - SA-5b3 ISO/IEC 27001:2022 - 7.5.3a ISO/IEC 27001:2022 - 7.5.3b ISO/IEC 27001:2022 - 7.5.3c ISO/IEC 27001:2022 - 7.5.3d MARS-E v2.2 - SA-5c MARS-E v2.2 - SA-5d MARS-E v2.2 - SA-5e NIST SP 800-53 R4 SA-5c[HML]{0} NIST SP 800-53 R4 SA-5d[HML]{0} NIST SP 800-53 R4 SA-5e[HML]{0} NIST SP 800-53 r5 - SA-5c NIST SP 800-53 r5 - SA-5d NY OHIP Moderate-Plus Security Baseline v5.0 - SA-5a2

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent, takes actions as defined when identified as nonexistent, protects documentation as required in accordance with the risk management strategy, and distributes documentation to at a minimum, the ISSO (or similar role within the organization).

Objective Name: 09.08 Exchange of Information

Control Objective:	Ensure the exchange of information within an organization, and with any external entity, is secured, protected, and carried out in compliance with relevant legislation and exchange agreements.

Control Reference: 09.s Information Exchange Policies and Procedures

Control Specification:	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication mediums.

Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA
Level 1 Implementation (example):	Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security (TLS) 1.2 or later; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TSL VPNs: SSL Portal VPN; SSL Tunnel VPN.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(02) (HIGH; MOD) Health Industry Cybersecurity Practices - 4.M.C Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(e)(1) HIPAA Security Rule - § 164.312(e)(2)(i) NIST Cybersecurity Framework v1.1 - PR.DS-2 PCI DSS v3.2.1 4.1 PCI DSS v3.2.1 4.1.1 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.215.2a
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? No Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No

Level 2 Regulatory Factors:	FedRAMP FISMA The Joint Commission v2016 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information High Low Moderate Supplemental
Level 2 Implementation (example):	An organization using electronic communication applications or systems for information exchange addresses the following: requirements (e.g., policies, standards) or guidelines are defined outlining acceptable use of electronic communication applications or systems; the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications; procedures are implemented for the use of wireless communications including an appropriate level of encryption; employee, contractor, and any other user's responsibilities are defined to not compromise the organization (e.g., through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.); the required use of cryptographic techniques to protect the confidentiality, integrity, and authenticity of covered information; the retention and disposal guidelines are defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and controls and restrictions are implemented associated with the forwarding of communications (e.g. automatic forwarding of electronic mail to external mail addresses). The organization establishes terms and conditions, consistent with any trust relationship established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems, and process, store or transmit organization-controlled information using external information systems.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.23 Banking Requirements - FFIEC IS v2016 A.6.24 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-17(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-20(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-15 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-15(01) (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 FedRAMP - AC-17(2)[H] FedRAMP - AC-17(2)[M] FedRAMP - AC-20(1)a[H] FedRAMP - AC-20(1)a[M] FedRAMP - AC-20(1)b[H] FedRAMP - AC-20(1)b[M] FedRAMP - AC-20(2)[H] FedRAMP - AC-20(2)[M] FedRAMP - AC-20a[H] FedRAMP - AC-20a[L] FedRAMP - AC-20a[M] FedRAMP - AC-20b[H] FedRAMP - AC-20b[L] FedRAMP - AC-20b[M] FedRAMP - MA-4 (6)[H] FedRAMP - SC-15a[H] FedRAMP - SC-15a[L] FedRAMP - SC-15a[M] FedRAMP - SC-15b[H] FedRAMP - SC-15b[L] FedRAMP - SC-15b[M] HIPAA Privacy Rule - 164.504(e)(3)(i)(A) HIPAA Privacy Rule - 164.504(e)(3)(i)(B) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(ii)(A) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) HIPAA Security Rule - § 164.308(a)(5)(ii)(A) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) IRS Pub 1075 - AC-17(2) IRS Pub 1075 - AC-20(2) IRS Pub 1075 - AC-20(5) IRS Pub 1075 - AC-20a1 IRS Pub 1075 - AC-20a2 IRS Pub 1075 - MA-4(6) IRS Pub 1075 - SA-9(3) IRS Pub 1075 - SC-15a IRS Pub 1075 - SC-15b ISO/IEC 27799:2016 13.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - AC-17(2) MARS-E v2.2 - AC-20(1)a MARS-E v2.2 - AC-20(1)b MARS-E v2.2 - AC-20(2) MARS-E v2.2 - AC-20b1 MARS-E v2.2 - AC-20b2

Level 2 Authoritative Source Mapping (Cont.):	MARS-E v2.2 - SC-15a MARS-E v2.2 - SC-15b NIST Cybersecurity Framework v1.1 - PR.AC-5 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-171 r2 - 3.1.13[a] NIST SP 800-171 r2 - 3.1.13[b] NIST SP 800-171 r2 - 3.1.21[a] NIST SP 800-171 r2 - 3.1.21[b] NIST SP 800-171 r2 - 3.1.21[c] NIST SP 800-171 r2 - 3.13.12[a] NIST SP 800-171 r2 - 3.13.12[b] NIST SP 800-171 r2 - 3.13.12[c] NIST SP 800-53 R4 AC-18a[HML]{0} NIST SP 800-53 R4 AC-20(1)[HM]{0} NIST SP 800-53 R4 AC-20(2)[HM]{0} NIST SP 800-53 R4 AC-20[HML]{0} NIST SP 800-53 R4 IA-9(1)[S]{1} NIST SP 800-53 R4 MA-4(4)b[S]{2} NIST SP 800-53 R4 MA-4(6)[S]{0} NIST SP 800-53 R4 SA-9(3)[S]{0} NIST SP 800-53 R4 SC-15a[HML]{0} NIST SP 800-53 R4 SC-15b[HML]{0} NIST SP 800-53 R4 SC-43[S]{0} NIST SP 800-53 r5 - AC-20(1)b NIST SP 800-53 r5 - AC-20(2) NIST SP 800-53 r5 - AC-20(5) NIST SP 800-53 r5 - AC-20a NIST SP 800-53 r5 - IA-5(9) NIST SP 800-53 r5 - MA-4(4)b NIST SP 800-53 r5 - MA-4(6) NIST SP 800-53 r5 - SA-9(3) NIST SP 800-53 r5 - SC-15 NIST SP 800-53 r5 - SC-43 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-17(2) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(1)b NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(2) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(2)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(2)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(2)[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20(2)[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20a1 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20a2 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-20a3 NY OHIP Moderate-Plus Security Baseline v5.0 - SC-15[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-15[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SC-15a NY OHIP Moderate-Plus Security Baseline v5.0 - SC-15b OCR Guidance for Unsecured PHI (1)(ii) PCI DSS v3.2.1 2.3 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(3) Supplemental Requirements - SR v6.4 45-0 The Joint Commission (v2016) - TJC IM.02.01.03, EP 1 The Joint Commission (v2016) - TJC IM.02.01.03, EP 5

Level Cloud Service Providers Implementation Requirements

Level Cloud Service Providers Implementation (example):	The cloud service provider uses secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and makes a document available to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.

	Cloud service providers use an industry-recognized virtualization platform and standard virtualization formats (e.g., Open Virtualization Format, OVF) to help ensure interoperability, and has documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization prohibits the use of external information systems including, but not limited to Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports. The organization establishes strict terms and conditions for the use of external information systems, which include, at a minimum: the types of applications that can be accessed from external information systems; the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; how other users of the external information system will be prevented from accessing federal information; the use of virtual private networking (VPN) and firewall technologies; the use of and protection against the vulnerabilities of wireless technologies; the maintenance of adequate physical security controls; the use of virus and spyware protection software; and how often the security capabilities of installed software are to be updated.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Unless approved by the Office of Safeguards, the organization prohibits: access to FTI from external information systems; use of organization-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems; and use of non-organization-owned information systems; system components; or devices to process, store, or transmit FTI. The organization notifies the Office of Safeguards 45 days prior to implementation that requires any non-organization-owned information system usage.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The organization maintains records of the basis used to authorize cross-border flows of personal data to a third country or international organization, which include but are not limited to: an adequacy decision by the EU Commission; the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available; binding corporate rules approved by the relevant supervisory authority; A court judgement or administrative decision of a third country if based on an international agreement between the third country and the EU; Or if one of the following conditions are met: the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; the transfer is necessary for important reasons of public interest; the transfer is necessary for the establishment, exercise or defense of legal claims; the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or Member State law for consultation are fulfilled in the particular case.

	Appropriate safeguards for cross-border flows of personal data include: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the Commission; standard data protection clauses adopted by a supervisory authority and approved by the Commission; an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. If authorized by the relevant supervisory authority, appropriate safeguards may also include contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization prohibits the use of external information systems, including but not limited to Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports by organizational users (staff and contractors within the organization) to store, access, transmit, or process sensitive information (such as FTI or Privacy Act protected information), unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. For non-organizational users (such as business partners), the Administering Entity organization establishes terms and conditions, consistent with CMS implementation guidance of HHS Regulation 45 C.F.R. § 115.260, and in compliance with legal data sharing agreements signed with CMS, for any trust relationships established with other organizations owning, operating, and/or maintaining external information systems.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization does not release information outside of the established system boundary unless: the receiving external organization (i.e., department, agency, or commercial entity not managed by CMS) provides information security and privacy safeguards commensurate with those implemented by CMS; and CMS-defined information security and privacy safeguards are used to validate the appropriateness of the information designated for release. For systems processing, storing, or transmitting PII (to include PHI), the organization does not release information outside of the established system boundary, unless the receiving organization or information system provides privacy and security controls commensurate with the PII confidentiality impact level of the PII being received, and controls UL-1 and UL-2 are used to validate the appropriateness of the information designated for release.

Control Reference: 09.t Exchange Agreements

Control Specification:	Agreements shall be established and implemented for the exchange of information and software between the organization and external parties.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	HITRUST De-ID Framework Texas Medical Records Privacy Act State of Nevada Security and Privacy of Personal Information
Level 1 Implementation (example):	Exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards, and solutions. The exchange and data sharing agreements also specify organization policies including: classification policy for the sensitivity of the business information; management responsibilities for controlling and notifying transmission, dispatch, and receipt; procedures for notifying sender of transmission, dispatch, and receipt; procedures to ensure traceability and non-repudiation; minimum technical standards for packaging and transmission; courier identification standards; responsibilities and liabilities in the event of information security incidents, such as loss of data; use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; technical standards for recording and reading information and software; any special controls that may be required to protect covered items, including cryptographic keys; and escrow agreements.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) COBIT 5 DS5.11 COBIT 5 DSS05.02 HITRUST De-ID Framework - De-ID Framework v1 Data Sharing Agreements: DSAs ISO/IEC 27799:2016 13.2.2

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	HITRUST De-ID Framework Texas Medical Records Privacy Act State of Nevada Security and Privacy of Personal Information
Level 2 Implementation (example):	The organization ensures policies, procedures, and standards are established and maintained to protect information and physical media in transit. Policies, procedures, and standards are referenced in such exchange agreements.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-01 (HIGH; MOD) HIPAA Security Rule - § 164.310(d)(1) ISO/IEC 27002:2022 - 5(14) ISO/IEC 27799:2016 13.2.2 NIST Cybersecurity Framework v1.1 - DE.CM-2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(c)

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization documents the interface characteristics between interconnecting information systems, and describes in the security plans for the respective systems when interconnecting systems have the same AO (or same primary operational IT infrastructure manager). When acquiring information systems, components, or services used to store, process, or transmit PHI, the organization, in consultation with the privacy office, ensures that (in addition to the requirements for PII) any necessary memorandum of understanding, memorandum of agreement, and other data sharing agreement are obtained.

Control Reference: 09.u Physical Media in Transit

Control Specification:	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundaries.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	PCI DSS v3.2.1 Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization protects physical media housing covered and/or confidential information from unauthorized disclosure or modification while in transit by the appropriate application of at least one of the following: use of locked containers; delivery by hand; tamper-evident packaging (which reveals any attempt to gain access); or splitting of the consignment into more than one delivery and dispatch by different routes.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.18(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) HIPAA Privacy Rule - 164.504(e)(2)(ii)(A) HIPAA Privacy Rule - 164.504(e)(2)(ii)(B) HIPAA Security Rule - § 164.312(c)(1) ISO/IEC 27799:2016 8.3.3

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA The Joint Commission v2016 Banking Requirements PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) GDPR State of Nevada Security and Privacy of Personal Information Supplemental
Level 2 Implementation (example):	Organizations protect information media being transported between sites through the use of: reliable transport or couriers that can be tracked; a list of authorized couriers agreed upon with management; checking/verification of identification of couriers; and packaging sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g., for software), such as by protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture, or electromagnetic fields. Media is encrypted when onsite unless physical security can be guaranteed. Media is always encrypted when offsite.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.18(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 MP-05(04) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-16 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-28 (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.310(d)(1) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(e)(2)(i) HIPAA Security Rule - § 164.312(e)(2)(ii) ISO/IEC 27799:2016 8.3.3 NIST SP 800-53 R4 SC-34(2)[S]{0} NIST SP 800-53 r5 - SC-34(2) PCI DSS v3.2.1 9.5 PCI DSS v3.2.1 9.6 PCI DSS v3.2.1 9.6.2 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.215.2b The Joint Commission (v2016) - TJC IM.02.01.03, EP 5
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization protects and controls digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography, tamper-evident packaging, if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or if shipped, trackable with receipt by commercial carrier. The organization maintains accountability for digital media and non-digital media containing CMS sensitive information during transport outside of controlled areas.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	All transportation or shipments of FTI (including electronic media or microfilm) are documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service is double-sealed. The inner envelope containing FTI transported through the mail or courier/messenger service is marked confidential. The outermost envelope must not be labeled as FTI or provide any indication that the contents contain FTI, since that may actually increase risk to the contents.

Control Reference: 09.v Electronic Messaging

Control Specification:	Information involved in electronic messaging shall be appropriately protected.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	

Level 1 System Factors:	
Level 1 Regulatory Factors:	CA Civil Code § 1798.81.5
Level 1 Implementation (example):	The organization has implemented Sender Policy Framework (SPF) by deploying SPF records in DNS, enabled receiver-side verification in mail servers to lower the chance of spoofed email messages, implemented DomainKeys Identified Mail (DKIM) to allow receiving servers to verify that email messages actually came from the organization, and implemented Domain-based Message Authentication, Reporting and Conformance (DMARC) to tell receiving servers to either quarantine or reject emails from the organization that don't pass SPF or DKIM. The organization uses an email filtering solution to recognize and block suspicious emails and unnecessary file types before they reach employee inboxes.
Level 1 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.17 CIS Controls v7.1 - CIS CSC v7.1 7.8 Health Industry Cybersecurity Practices - 1.M.A Health Industry Cybersecurity Practices - 1.S.A

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)? No
Level 2 Regulatory Factors:	DirectTrust FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The organization ensures legal considerations, including requirements for electronic signatures, are addressed. Approvals are obtained prior to using external public services, including instant messaging or file sharing.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-CMS-1 (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 Health Industry Cybersecurity Practices - 1.M.C Health Industry Cybersecurity Practices - 4.S.B HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(2)(i) HIPAA Security Rule - § 164.312(e)(2)(ii) IRS Pub 1075 - PL-4(IRS-1) ISO/IEC 27002:2022 - 8(5) ISO/IEC 27799:2016 13.2.3 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - SC-ACA-1 NIST Cybersecurity Framework v1.1 - ID.GV-3 NIST Cybersecurity Framework v1.1 - PR.DS-2 PCI DSS v3.2.1 4.2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(3)
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	If FTI is allowed to be included within emails or email attachments, the organization only transmits FTI to an authorized recipient. Email transmissions that contain FTI are encrypted using a FIPS 140-2 validated mechanism.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	Email and any attachment that contains sensitive information when transmitted inside and outside of HHS premises are encrypted using the user's personal identity verification (PIV) card when possible. If PIV encryption is not feasible, a FIPS 140-2 validated solution must be employed. Password protection of files is recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions. Password and/or encryption keys are not included in the same email that contains sensitive information or in separate email, and password/encryption key is provided to the recipient separately via text message, verbally, or other out-of-band solution.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization ensures the following basic email protections are implemented: real-time blackhole lists; removal of open relays; X-HEADERS; and distributed checksum clearinghouse (DCC). Email messages are scored by each of the basic email protections and automated actions are executed to either deliver, quarantine, or block the message based on organization defined thresholds.

Control Reference: 09.w Interconnected Business Information Systems

Control Specification:	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	A security baseline is documented and implemented for interconnected systems.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DSS05.02 COBIT 5 DSS05.03 Health Industry Cybersecurity Practices - 9.M.A Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(i) Veterans Affairs Cybersecurity Program Directive 6500 - c(1)(d)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Moderate Supplemental

Level 2 Implementation (example):	The organization authorizes and approves connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system. The organization documents, for each internal connection, the interface characteristics, security requirements, information communicated, and security and business implications. Security and business implications are addressed for interconnecting business information assets which include known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the organization, restricting access to diary information relating to selected individuals (e.g., personnel working on sensitive projects), and vulnerabilities of information in business communication systems (e.g., recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail). Other requirements and controls linked to interconnected business systems include the separation of operational systems from interconnected system, retention and back-up of information held on the system, and fallback requirements and arrangements.
Level 2 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-09 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DS5.11 COBIT 5 DSS05.02 FedRAMP - CA-9a[H] FedRAMP - CA-9a[L] FedRAMP - CA-9a[M] FedRAMP - CA-9b[H] FedRAMP - CA-9b[L] FedRAMP - CA-9b[M] HIPAA Security Rule - § 164.308(a)(1)(ii)(B) IRS Pub 1075 - CA-9a IRS Pub 1075 - CA-9b ISO/IEC 27799:2016 13.1.3 MARS-E v2.2 - CA-9a MARS-E v2.2 - CA-9b NIST Cybersecurity Framework v1.1 - DE.AE-1 NIST Cybersecurity Framework v1.1 - ID.AM-3 NIST SP 800-53 R4 AC-4[HM]{1} NIST SP 800-53 R4 CA-3(4)[S]{0} NIST SP 800-53 R4 SC-42(2)[S]{0} NIST SP 800-53 R4 SC-42(3)[S]{0} NIST SP 800-53 R4 SC-42[S]{0} NIST SP 800-53 r5 - AC-4 NIST SP 800-53 r5 - CA-9a NIST SP 800-53 r5 - CA-9b NIST SP 800-53 r5 - SC-42 NIST SP 800-53 r5 - SC-42(2) NY OHIP Moderate-Plus Security Baseline v5.0 - CA-9a NY OHIP Moderate-Plus Security Baseline v5.0 - CA-9b PCI DSS v3.2.1 1.2

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	The organization reviews the continued need for each internal connection of information system components or classes of components to the information system at least annually. The information system terminates internal system connections after organization-defined conditions.

Objective Name: 09.09 On-line Transactions

Control Objective:	Ensure the security of on-line transactions.

Control Reference: 09.x Electronic Commerce Services

Control Specification:	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure or modification.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services? No
Level 1 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	A documented agreement is committed and maintained for electronic commerce arrangements between trading partners including the agreed terms of trading and details of authorization. Other agreements with information service and value added network providers are also required.
Level 1 Authoritative Source Mapping:	HIPAA Privacy Rule - 164.504(e)(1)(i) ISO/IEC 27799:2016 14.1.2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records

Level 2 System Factors:	Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services? No
Level 2 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The confidentiality and integrity for electronic commerce is maintained by: ensuring the level of confidence each party requires in each other's claimed identity (e.g., through authentication); ensuring the authorization processes associated with who may set prices, issue or sign key trading documents; ensuring that trading partners are fully informed of their authorizations; determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts (e.g. associated with tendering and contract processes); ensuring the level of trust required in the integrity of advertised price lists; ensuring the confidentiality of any covered data or information; ensuring the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts; ensuring the degree of verification appropriate to check payment information supplied by a customer; selecting the most appropriate settlement form of payment to guard against fraud; ensuring the level of protection required to maintain the confidentiality and integrity of order information; ensuring avoidance of loss or duplication of transaction information; ensuring liability associated with any fraudulent transactions; and ensuring insurance requirements. Attacks of the host(s) used for electronic commerce are addressed to provide resilient service(s).
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-10 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08(01) (HIGH; MOD) COBIT 5 DS5.11 Health Industry Cybersecurity Practices - 2.M.A HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(c)(2) HIPAA Security Rule - § 164.312(e)(2)(i) ISO/IEC 27799:2016 14.1.2 NIST Cybersecurity Framework v1.1 - ID.GV-3 NIST SP 800-53 r5 - CP-9(8) Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(i)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The information system protects against an individual (or process acting on behalf of an individual) from falsely denying the performance of a particular action.

Control Reference: 09.y On-line Transactions

Control Specification:	Information involved in online transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL).
Level 1 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 1.M.C ISO/IEC 27799:2016 14.1.3 NIST SP 800-53 r5 - SC-16(3)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? No
Level 2 Regulatory Factors:	GDPR
Level 2 Implementation (example):	Data involved in electronic commerce and online transactions are checked to determine if it contains covered information. Security is maintained through all aspects of the transaction, ensuring that: user credentials of all parties are valid and verified; the transaction remains confidential; and privacy associated with all parties involved is retained.
Level 2 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-10 (HIGH) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(1) HIPAA Security Rule - § 164.312(e)(2)(ii) ISO/IEC 27799:2016 14.1.3 Legacy Inheritance Support - L.I.S.

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	GDPR
Level 3 Implementation (example):	The protocols used for communications are enhanced to address any new vulnerability. The updated versions are adopted as soon as possible.
Level 3 Authoritative Source Mapping:	ISO/IEC 27799:2016 14.1.3
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	All Internet transmissions in a data warehouse, and all sessions are encrypted appropriately. Transaction data is swept from the web server(s) at frequent intervals, consistent with good system performance, and removed to a secured server behind the firewalls to minimize risk.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization transmits access authorization information using cryptographic mechanisms to systems that enforce access control decisions when the authorization processes and access control decisions occur in separate parts of systems or in separate systems.

Control Reference: 09.z Publicly Available Information

Control Specification:	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization designates individuals authorized to post information onto a publicly accessible information system, and trains these individuals to ensure that publicly accessible information does not contain nonpublic information.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-22 (HIGH; MOD) COBIT 5 DS7.2 COBIT 5 DSS06.03 FedRAMP - AC-22a[H] FedRAMP - AC-22a[L] FedRAMP - AC-22a[M] FedRAMP - AC-22b[H] FedRAMP - AC-22b[L] FedRAMP - AC-22b[M] IRS Pub 1075 - AC-22a IRS Pub 1075 - AC-22b MARS-E v2.2 - AC-22a MARS-E v2.2 - AC-22b NIST SP 800-171 r2 - 3.1.22[a] NIST SP 800-53 R4 AC-22a[HML]{0} NIST SP 800-53 R4 AC-22b[HML]{0} NIST SP 800-53 r5 - AC-22a NIST SP 800-53 r5 - AC-22b NY OHIP Moderate-Plus Security Baseline v5.0 - AC-22a NY OHIP Moderate-Plus Security Baseline v5.0 - AC-22b

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	The organization ensures that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications. The organization reviews the proposed content of information prior to posting onto the publicly accessible information system, and on a recurring bi-weekly basis to ensure non-public information is not included. The organization removes nonpublic information if discovered.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC8.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-22 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-CMS-2 (HIGH; MOD) FedRAMP - AC-22c[H] FedRAMP - AC-22c[L] FedRAMP - AC-22c[M] HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(e)(2)(i) IRS Pub 1075 - AC-22c MARS-E v2.2 - AC-22c MARS-E v2.2 - AC-22d NIST Cybersecurity Framework v1.1 - DE.CM-8 NIST Cybersecurity Framework v1.1 - PR.AC-5 NIST Cybersecurity Framework v1.1 - PR.DS-6 NIST SP 800-171 r2 - 3.1.22[b] NIST SP 800-171 r2 - 3.1.22[c] NIST SP 800-171 r2 - 3.1.22[d] NIST SP 800-171 r2 - 3.1.22[e] NIST SP 800-53 R4 AC-22c[HML]{0} NIST SP 800-53 R4 AC-22d[HML]{0} NIST SP 800-53 r5 - AC-22c NIST SP 800-53 r5 - AC-22d NY OHIP Moderate-Plus Security Baseline v5.0 - AC-22c NY OHIP Moderate-Plus Security Baseline v5.0 - AC-22d NY OHIP Moderate-Plus Security Baseline v5.0 - AC-3[IS.2]

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA Supplemental
Level 3 Implementation (example):	Software, data, and other information requiring a high level of integrity being made available on a publicly available system is protected by appropriate mechanisms, including digital signatures.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-05(02) (HIGH; MOD) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(c)(2) ISO/IEC 27799:2016 14.1.2 NIST SP 800-53 R4 SI-7(6)[S]{2} NIST SP 800-53 r5 - SI-7(6)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	Websites are operated within the restrictions addressed in: OMB directives M-10-22 “Guidance for Online Use of Web Measurement and Customization Technologies”; M-10-23 “Guidance for Agency Use of Third-Party websites and Applications”; and applicable CMS and DHHS directives and instruction. The organization monitors the CMS and DHHS security programs to determine if there are any modified directives and instruction.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization reviews the content on the publicly accessible information system for nonpublic information at least quarterly and removes such information, if discovered.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization: designates individuals authorized to post information onto a publicly accessible information system; trains authorized individuals to ensure that publicly accessible information does not contain FTI; reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included; and reviews the content on the publicly accessible information system for FTI, at a minimum, quarterly and remove such information, if discovered.

Objective Name: 09.10 Monitoring

Control Objective:	Ensure information security events are monitored and recorded to detect unauthorized information processing activities in compliance with all relevant legal requirements.

Control Reference: 09.aa Audit Logging	
Control Specification:	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust HITRUST De-ID Framework Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate Supplemental
Level 1 Implementation (example):	Audit records include a unique user ID, unique data subject ID (if applicable), function performed, and date/time the event was performed. Retention policies for audit logs are specified by the organization and the audit logs are retained accordingly.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(b) 21 CFR Part 11.10(e) 23 NYCRR 500 - 500.06(b) AICPA Trust Services Criteria - AICPA 2017 CC2.1 Banking Requirements - FFIEC IS v2016 A.6.21(b) Banking Requirements - FFIEC IS v2016 A.6.22(f) Banking Requirements - FFIEC IS v2016 A.6.27(a) Banking Requirements - FFIEC IS v2016 A.6.35 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-08 (HIGH; MOD) COBIT 5 DSS05.04 Health Industry Cybersecurity Practices - 4.M.C Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.312(b) HIPAA Security Rule - § 164.316(b)(1)(ii) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Audit Logging/Monitoring: General HITRUST De-ID Framework - De-ID Framework v1 Retention: Data Retention Policy ISO/IEC 27799:2016 12.4.1 NIST Cybersecurity Framework v1.1 - PR.PT-1 NIST SP 800-171 r2 - 3.3.2[a] NIST SP 800-171 r2 - 3.3.2[b] NIST SP 800-53 R4 AU-14(2)[S]{0} NIST SP 800-53 R4 AU-14[S]{2} NIST SP 800-53 R4 AU-8[HML]{2} NIST SP 800-53 r5 - AU-14a NIST SP 800-53 r5 - AU-8 OCR Audit Protocol (2016) 164.308(a)(5)(ii)(C) PCI DSS v3.2.1 10.3.1 PCI DSS v3.2.1 10.3.2 PCI DSS v3.2.1 10.3.3 PCI DSS v3.2.1 10.3.5 PCI DSS v3.2.1 10.3.7 Supplemental Requirements - SR v6.4 28.2-0 Supplemental Requirements - SR v6.4 28a-0 Supplemental Requirements - SR v6.4 28b-0 Supplemental Requirements - SR v6.4 45b.3-0 Supplemental Requirements - SR v6.4 7b.6-0 Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(b)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	DirectTrust HITRUST De-ID Framework 23 NYCRR 500 Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate Supplemental

Level 2 Implementation (example):	A secure audit record is created each time a user accesses, creates, updates, or deletes covered and/or confidential information via the system. The activities of privileged users (administrators, operators, etc.) include the success/failure of the event, time the event occurred, information about the event (e.g., files handled) or failure (e.g., error occurred and corrective action taken), the account or administrator involved, and which processes were involved.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(b) 21 CFR Part 11.10(e) Banking Requirements - FFIEC IS v2016 A.6.20(d) Banking Requirements - FFIEC IS v2016 A.6.21(b) Banking Requirements - FFIEC IS v2016 A.6.22(f) Banking Requirements - FFIEC IS v2016 A.6.27(a) Banking Requirements - FFIEC IS v2016 A.6.35 CIS Controls v7.1 - CIS CSC v7.1 14.9 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(09) (HIGH; MPD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-11 (HIGH; MOD) COBIT 5 DSS05.04 FedRAMP - AU-11[H] FedRAMP - AU-11[L] FedRAMP - AU-11[M] Health Industry Cybersecurity Practices - 3.S.A HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.312(b) HITRUST HITRUST De-ID Framework - De-ID Framework v1 Audit Logging/Monitoring: General HITRUST De-ID Framework - De-ID Framework v1 Retention: Data Retention Policy ISO/IEC 27799:2016 12.4.1 ISO/IEC 27799:2016 12.4.2 ISO/IEC 27799:2016 12.4.3 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST Cybersecurity Framework v1.1 - RS.IM-1 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST SP 800-53 R4 AC-9(3)[S]{0} NIST SP 800-53 R4 AU-10(1)b[S]{0} NIST SP 800-53 R4 AU-10[H]{1} NIST SP 800-53 R4 AU-11[HML]{0} NIST SP 800-53 R4 AU-2(3)[HM]{0} NIST SP 800-53 R4 AU-2c[HML]{0} NIST SP 800-53 R4 AU-2d[HML]{0} NIST SP 800-53 R4 AU-6(8)[S]{2} NIST SP 800-53 R4 SA-12(14)[S]{0} NIST SP 800-53 R4 SI-10(1)c[S]{0} NIST SP 800-53 r5 - AC-9(3) NIST SP 800-53 r5 - AU-10 NIST SP 800-53 r5 - AU-10(1)b NIST SP 800-53 r5 - AU-11 NIST SP 800-53 r5 - AU-2c NIST SP 800-53 r5 - AU-2d NIST SP 800-53 r5 - AU-2e NIST SP 800-53 r5 - AU-3(3) NIST SP 800-53 r5 - AU-6(8) NIST SP 800-53 r5 - CA-7(6) NIST SP 800-53 r5 - SI-10(1)c NIST SP 800-53 r5 - SR-4(1) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-6(9) NY OHIP Moderate-Plus Security Baseline v5.0 - AU-11 PCI DSS v3.2.1 10.2

Level 2 Authoritative Source Mapping (Cont.):	PCI DSS v3.2.1 10.2.1 PCI DSS v3.2.1 10.2.2 PCI DSS v3.2.1 10.2.4 PCI DSS v3.2.1 10.2.7 PCI DSS v3.2.1 10.3.1 PCI DSS v3.2.1 10.3.2 PCI DSS v3.2.1 10.3.3 PCI DSS v3.2.1 10.3.4 PCI DSS v3.2.1 10.3.5 PCI DSS v3.2.1 10.3.6 PCI DSS v3.2.1 10.5 PCI DSS v3.2.1 10.7 Supplemental Requirements - SR v6.4 28.1-0
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 3 Implementation (example):	Audit logs are maintained for account management activities, system/server shutdown and reboot, system/server alerts and errors, application/system shutdown and reboot, application errors and modifications, file changes (create, update, delete), security policy changes, configuration changes, modification to sensitive information, read access to sensitive information, and printing of sensitive information. The information system generates audit records containing the following detailed information: filename accessed; program or command used to initiate the event; source addresses; and destination addresses.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(e) AICPA Trust Services Criteria - AICPA 2017 C1.2 CIS Controls v7.1 - CIS CSC v7.1 4.8 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06(09) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-03(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-12 (HIGH; MOD) COBIT 5 DSS05.04 FedRAMP - AC-2(4)[H] FedRAMP - AC-2(4)[M] HIPAA Privacy Rule - 164.504(e)(2)(ii)(G) HIPAA Privacy Rule - 164.528(b)(2)(i) HIPAA Privacy Rule - 164.528(b)(2)(ii) HIPAA Privacy Rule - 164.528(b)(3)(ii) HIPAA Privacy Rule - 164.528(b)(3)(iii) HIPAA Security Rule - § 164.312(b) HITRUST IRS Pub 1075 - AC-2(4) ISO/IEC 27799:2016 12.4.1 MARS-E v2.2 - AC-2(4) MARS-E v2.2 - AU-3(1)a1 MARS-E v2.2 - AU-3(1)a2 MARS-E v2.2 - AU-3(1)a3 MARS-E v2.2 - AU-3a NIST Cybersecurity Framework v1.1 - PR.AC-1 NIST Cybersecurity Framework v1.1 - PR.PT-1 NIST SP 800-53 R4 AC-2(4)[HM]{0} NIST SP 800-53 R4 AU-14[S]{3} NIST SP 800-53 R4 AU-3(1)[HM]{0} NIST SP 800-53 r5 - AC-2(4) NIST SP 800-53 r5 - AU-14a NIST SP 800-53 r5 - AU-3(1) NY OHIP Moderate-Plus Security Baseline v5.0 - AC-2(4) NY OHIP Moderate-Plus Security Baseline v5.0 - AU-3(1)
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization logs all URL requests from each of the organization’s systems, whether onsite or on a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems. The organization enables system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	Audit inspection reports, including a record of corrective actions, are retained by the organization for a minimum of three years from the date the inspection was completed. Audit records are compiled from multiple components throughout the system into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five minutes.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The service provider retains audit records on-line for at least 90 days and further preserves audit records off-line for a period that is in accordance with National Archives and Records Administration (NARA) requirements. Audit logging and monitoring is coordinated between the service provider and the organization and documented. Audit logging and monitoring is accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO).
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization's audit record generation capability audits: logons; logoffs; changes of password; all system administrator commands while logged on as system administrator; switching accounts; running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS); creation or modification of super-user groups; a subset of security administrator commands, while logged on in the security administrator role; a subset of system administrator commands, while logged on in the user role; clearing of the audit log file; startup of audit functions; and shutdown of audit functions. The organization's audit record generation capability audits: use of identification and authentication mechanisms (e.g., user ID and password); changes of file or user permissions or privileges (e.g., use of suid/guid, chown, su); remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN); all dial-in access to the system; changes made to applications by batch file; changes made to databases by batch file; application-critical record changes; changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); all system and data interactions concerning FTI; additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards Website.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject. The organization archives old audit records for ten years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	A service provider protects each organization's hosted environment and data by ensuring logging and audit trails are enabled, unique to each organization's (customer's) cardholder data environment, and consistent with PCI DSS v3.1 Requirement 10.
Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation (example):	The organization maintains audit records designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the organization for three years.
Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation (example):	All records concerning cybersecurity events are maintained for at least five years from the date of the event and are available for inspection.

Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization implements a centralized mechanism to log privileged activities, including the use of privileged accounts and grants to privileged groups. The organization develops alerting rules and investigation procedures to review suspicious activities.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The information system performs an integrity check of software, firmware, and information daily and at system startup.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization develops, documents, and disseminates to organization-defined personnel or roles an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. The organization reviews and updates the current audit and accountability policy and procedures within organization-defined frequency. The information system audits changes to security and privacy attributes for information in storage, in process, and in transmission.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization maintains, audits, and monitors an electronic audit log which contains an entry when a record or part of a record of personal health information that is accessible by electronic means is viewed, handled, modified or otherwise dealt with. The organization, for every instance in which a record or part of a record of PHI that is accessible by electronic means is viewed, handled, modified or otherwise dealt with, maintains electronic audit logs containing the identity of the individual to whom the PHI relates, the date and time, the identity of all persons who viewed, handled, modified, or otherwise dealt with the PHI, and the type of information that was viewed, handled, modified or otherwise dealt with.

Control Reference: 09.ab Monitoring System Use

Control Specification:	Procedures for monitoring use of information processing systems and facilities shall be established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.

Level 1 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 3.M.C Health Industry Cybersecurity Practices - 9.M.A HIPAA Security Rule - § 164.308(a)(1)(ii)(D) NIST Cybersecurity Framework v1.1 - PR.PT-1 OCR Audit Protocol (2016) 164.308(a)(1)(ii)(D)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	DirectTrust FTC Red Flags Rule (16 CFR 681) 23 NYCRR 500 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act High Low Moderate Supplemental
Level 2 Implementation (example):	The organization complies with all relevant legal requirements applicable to its monitoring of authorized access and unauthorized access attempts. Information systems containing covered and/or confidential information are provided with automated tools for monitoring system events, detecting attacks and analyzing logs and audit trails to support the identification of access to and modification of covered and/or confidential records by a given user over a given period of time. Monitoring devices are deployed at strategic and ad hoc locations to track specific transactions and the impact of security changes to information systems. The organization reviews physical access logs weekly and upon occurrence of security incidents involving physical security. The organization deploys NetFlow-style collection and analysis to DMZ network flows to detect anomalous activity.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.2 AICPA Trust Services Criteria - AICPA 2017 CC2.1 AICPA Trust Services Criteria - AICPA 2017 CC7.2 Banking Requirements - FFIEC IS v2016 A.6.20(d) Banking Requirements - FFIEC IS v2016 A.6.21(f) Banking Requirements - FFIEC IS v2016 A.6.21(g) Banking Requirements - FFIEC IS v2016 A.6.22(f) Banking Requirements - FFIEC IS v2016 A.6.35 Banking Requirements - FFIEC IS v2016 A.6.35(c) Banking Requirements - FFIEC IS v2016 A.8.1(h) Banking Requirements - FFIEC IS v2016 A.8.5(a) CIS Controls v7.1 - CIS CSC v7.1 12.5 CIS Controls v7.1 - CIS CSC v7.1 12.8 CIS Controls v7.1 - CIS CSC v7.1 13.5 CIS Controls v7.1 - CIS CSC v7.1 15.10 CIS Controls v7.1 - CIS CSC v7.1 16.12 CIS Controls v7.1 - CIS CSC v7.1 16.13 CIS Controls v7.1 - CIS CSC v7.1 6.2 CIS Controls v7.1 - CIS CSC v7.1 8.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-07(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-06 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PE-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04(02) (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 FedRAMP - PE-6a[H] FedRAMP - PE-6a[L] FedRAMP - PE-6a[M] FedRAMP - PE-6c[H] FedRAMP - PE-6c[L] FedRAMP - PE-6c[M] FedRAMP - SI-4c[H] FedRAMP - SI-4ci[L] FedRAMP - SI-4ci[M] FedRAMP - SI-4cii[L] FedRAMP - SI-4cii[M] FTC Red Flags Rule (16 CFR 681) - 681.A3.b HIPAA Security Rule - § 164.308(a)(1)(ii)(D) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(5)(ii)(C) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.312(b) HITRUST De-ID Framework - De-ID Framework v1 Audit Logging/Monitoring: General IRS Pub 1075 - 2.B.3.3(5) IRS Pub 1075 - PE-6a IRS Pub 1075 - PE-6c IRS Pub 1075 - SI-4c1 IRS Pub 1075 - SI-4c2 IRS Pub 1075 - SI-4d ISO/IEC 27002:2022 - 8(16)

Level 2 Authoritative Source Mapping (Cont.):	ISO/IEC 27799:2016 12.4.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PE-6a MARS-E v2.2 - PE-6b MARS-E v2.2 - PE-6c MARS-E v2.2 - SI-4a1 MARS-E v2.2 - SI-4c1 MARS-E v2.2 - SI-4c2 NIST Cybersecurity Framework v1.1 - DE.AE-2 NIST Cybersecurity Framework v1.1 - DE.AE-3 NIST Cybersecurity Framework v1.1 - DE.CM-3 NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - DE.DP-2 NIST Cybersecurity Framework v1.1 - ID.GV-3 NIST Cybersecurity Framework v1.1 - RS.RP-1 NIST SP 800-171 r2 - 3.14.7[a] NIST SP 800-171 r2 - 3.14.7[b] NIST SP 800-171 r2 - 3.3.6[a] NIST SP 800-171 r2 - 3.3.6[b] NIST SP 800-53 R4 AC-4(9)[S]{0} NIST SP 800-53 R4 AU-6(1)[HM]{0} NIST SP 800-53 R4 AU-6(6)[H]{1} NIST SP 800-53 R4 AU-6a[HML]{0} NIST SP 800-53 R4 AU-7[HM]{0} NIST SP 800-53 R4 PE-6c[HML]{0} NIST SP 800-53 R4 SI-4(20)[S]{0} NIST SP 800-53 R4 SI-4c[HML]{0} NIST SP 800-53 R4 SI-4f[HML]{0} NIST SP 800-53 r5 - AC-2g NIST SP 800-53 r5 - AC-4(9) NIST SP 800-53 r5 - AU-6(6) NIST SP 800-53 r5 - AU-6a NIST SP 800-53 r5 - IR-4(13) NIST SP 800-53 r5 - PE-6c NIST SP 800-53 r5 - SI-4(20) NIST SP 800-53 r5 - SI-4c NIST SP 800-53 r5 - SI-4d NIST SP 800-53 r5 - SI-4f NY OHIP Moderate-Plus Security Baseline v5.0 - PE-6b NY OHIP Moderate-Plus Security Baseline v5.0 - PE-6c NY OHIP Moderate-Plus Security Baseline v5.0 - PM-14[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-32 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-32[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(23)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4c1 NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4c2 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(h) Supplemental Requirements - SR v6.4 17.2-1 Supplemental Requirements - SR v6.4 17.8-0 Supplemental Requirements - SR v6.4 43-0 Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(a) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(b) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(d)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	

Level 3 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 3 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	Automated systems are used to review monitoring activities on a daily basis for those servers that perform security functions (e.g., IDS/IPS) for: all security events; logs of all critical system components; and logs of all servers that perform security functions like intrusion detection system (IDS), intrusion prevention system (IPS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). System records are reviewed daily for initialization sequences, log-ons and errors, system processes and performance, and system resources utilization. The results of system record reviews are used to determine anomalies on demand. The organization ensures automated alerts are generated for technical personnel to review and analyze, and suspicious activity or suspected violations are investigated as an integrated part of the organization’s formal incident response and investigations program.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC2.1 AICPA Trust Services Criteria - AICPA 2017 CC7.2 Banking Requirements - FFIEC IS v2016 A.6.35(d) Banking Requirements - FFIEC IS v2016 A.8.1(h) CIS Controls v7.1 - CIS CSC v7.1 6.6 CIS Controls v7.1 - CIS CSC v7.1 6.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-06(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-06(05) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-06(06) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-07(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-03 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04(04) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-04(05) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-07(02) (HIGH) COBIT 5 DS5.9 COBIT 5 DSS05.01 COBIT 5 DSS05.07 FedRAMP - AU-12a[H] FedRAMP - AU-12a[L] FedRAMP - AU-12a[M] FedRAMP - AU-6(3)[H] FedRAMP - AU-6(3)[M] FedRAMP - AU-6(4)[H] FedRAMP - AU-7(1)[H] FedRAMP - AU-7(1)[M] FedRAMP - SI-4(16)[H] FedRAMP - SI-4(16)[M] FedRAMP - SI-4(2)[H] FedRAMP - SI-4(2)[M] FedRAMP - SI-4(4)[H] FedRAMP - SI-4(4)[M] Health Industry Cybersecurity Practices - 9.L.B HIPAA Security Rule - § 164.308(a)(1)(ii)(D) HIPAA Security Rule - § 164.308(a)(5)(ii)(B) HIPAA Security Rule - § 164.308(a)(5)(ii)(C) HIPAA Security Rule - § 164.312(b) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(c)(2) HIPAA Security Rule - § 164.312(e)(2)(i) HITRUST De-ID Framework - De-ID Framework v1 Audit Logging/Monitoring: Aberrant and Inappropriate Use IRS Pub 1075 - AU-2b IRS Pub 1075 - AU-6(3) IRS Pub 1075 - AU-6(9) IRS Pub 1075 - MA-4(1)b IRS Pub 1075 - SI-4(12) IRS Pub 1075 - SI-4(2) IRS Pub 1075 - SI-4(4)b MARS-E v2.2 - AU-6(3) MARS-E v2.2 - AU-7(1) MARS-E v2.2 - SC-7a MARS-E v2.2 - SI-4(1) MARS-E v2.2 - SI-4(2) MARS-E v2.2 - SI-4(4) MARS-E v2.2 - SI-4(5)a

Level 3 Authoritative Source Mapping (Cont.):	NIST Cybersecurity Framework v1.1 - DE.AE-2 NIST Cybersecurity Framework v1.1 - DE.AE-3 NIST Cybersecurity Framework v1.1 - DE.AE-4 NIST Cybersecurity Framework v1.1 - DE.CM-4 NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - DE.DP-4 NIST Cybersecurity Framework v1.1 - PR.PT-1 NIST Cybersecurity Framework v1.1 - RS.AN-1 NIST SP 800-53 R4 AC-20(4)[S]{1} NIST SP 800-53 R4 AU-12(2)[S]{0} NIST SP 800-53 R4 AU-12a[HML]{0} NIST SP 800-53 R4 AU-12b[HML]{0} NIST SP 800-53 R4 AU-2a[HML]{0} NIST SP 800-53 R4 AU-2b[HML]{0} NIST SP 800-53 R4 AU-3(2)[H]{0} NIST SP 800-53 R4 AU-5(2)[H]{0} NIST SP 800-53 R4 AU-6(3)[HM]{0} NIST SP 800-53 R4 AU-6(4)[S]{0} NIST SP 800-53 R4 AU-6(7)[S]{0} NIST SP 800-53 R4 AU-6(9)[S]{0} NIST SP 800-53 R4 AU-7(2)[S]{0} NIST SP 800-53 R4 SA-18(2)[S]{2} NIST SP 800-53 R4 SI-3(8)[S]{2} NIST SP 800-53 R4 SI-4(13)[S]{0} NIST SP 800-53 R4 SI-4(16)[S]{0} NIST SP 800-53 R4 SI-4(17)[S]{1} NIST SP 800-53 R4 SI-4(2)[HM]{0} NIST SP 800-53 R4 SI-4(3)[S]{0} NIST SP 800-53 R4 SI-4(4)[HM]{0} NIST SP 800-53 R4 SI-4b[HML]{0} NIST SP 800-53 R4 SI-7(8)[S]{0} NIST SP 800-53 r5 - AC-16(3) NIST SP 800-53 r5 - AU-12(2) NIST SP 800-53 r5 - AU-12a NIST SP 800-53 r5 - AU-12b NIST SP 800-53 r5 - AU-2a NIST SP 800-53 r5 - AU-2b NIST SP 800-53 r5 - AU-5(2) NIST SP 800-53 r5 - AU-6(3) NIST SP 800-53 r5 - AU-6(4) NIST SP 800-53 r5 - AU-6(7) NIST SP 800-53 r5 - AU-6(9) NIST SP 800-53 r5 - RA-3(4) NIST SP 800-53 r5 - SC-48(1) NIST SP 800-53 r5 - SI-3(8) NIST SP 800-53 r5 - SI-4(13) NIST SP 800-53 r5 - SI-4(16) NIST SP 800-53 r5 - SI-4(17) NIST SP 800-53 r5 - SI-4(2) NIST SP 800-53 r5 - SI-4(3) NIST SP 800-53 r5 - SI-4(4)b NIST SP 800-53 r5 - SI-4b NIST SP 800-53 r5 - SI-7(8) NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(1)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(1)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(1)[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(3) NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(3)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(3)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(3)[IS.1c]

Level 3 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - AU-6(4) NY OHIP Moderate-Plus Security Baseline v5.0 - AU-7(1) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[PHI.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[PHI.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[PHI.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(2)[PHI.2] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4(4)b NY OHIP Moderate-Plus Security Baseline v5.0 - SI-4d PCI DSS v3.2.1 10.6 PCI DSS v3.2.1 10.6.1 PCI DSS v3.2.1 10.6.3 PCI DSS v3.2.1 11.5 Supplemental Requirements - SR v6.4 32a-1 Supplemental Requirements - SR v6.4 32a-2 Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(f) Veterans Affairs Cybersecurity Program Directive 6500 - d(3)(b)
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization profiles each user's typical account usage by determining normal time-of-day access and access duration. The organization generates reports that indicate users who have logged in during unusual hours, that indicate users who have exceeded their normal login duration, and which includes flagging the use of the user's credentials from a computer other than computers on which the user generally works. The organization employs automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events are sent to enterprise anti-malware administration tools and event log servers.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization monitors events on the information system to detect information system attacks in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure. The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	Coordination between service provider and consumer is documented and accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO). In multi-tenant environments, capability and means for providing review, analysis, and reporting to the consumer for data pertaining to the consumer is documented. The organization reviews audit records at least once every seven days for unusual, unexpected, or suspicious behavior.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	All requests for return information, including receipt and/or disposal of returns or return information, is maintained in a log.

	The organization reports findings from the review and analysis of information system audit records according to the organization incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 1.8, Reporting Improper Inspections or Disclosures.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization reviews network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a 24 hour period. The organization generates alerts for technical personnel review and assessment. The organization uses automated utilities to review audit records at least once every seven days for unusual, unexpected, or suspicious behavior.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization reviews, at least daily, the logs of all system components that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD), or that could impact the security of CHD and/or SAD. When being assessed as a service provider, the organization implements a process for the timely detection and reporting of failures of critical security control systems.
Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation (example):	Information collected from multiple sources is aggregated and reviewed.
Level Supplemental Requirements Implementation Requirements	
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization monitors systems, appliances, devices, applications, and databases. The information system, when supported by the operating system, notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization tests its monitoring and detection processes periodically, remediates deficiencies, and improves its processes. The organization establishes and maintains a security operations center capability that facilitates 24/7 incident detection and response.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization establishes and maintains a security operations center capability that facilitates incident detection and response. The organization configures DLP systems to crawl known public websites for sensitive information.

Control Reference: 09.ac Protection of Log Information

Control Specification:	Logging systems and log information shall be protected against tampering and unauthorized access.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	High Low Moderate Supplemental
Level 1 Implementation (example):	Access to audit trails / logs is safeguarded from unauthorized access and use.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.21(b) Banking Requirements - FFIEC IS v2016 A.6.35(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-09 (HIGH; MOD) IRS Pub 1075 - 2.A.2(3) ISO/IEC 27799:2016 12.4.2 ISO/IEC 27799:2016 12.4.3 NIST SP 800-171 r2 - 3.3.8[a] NIST SP 800-171 r2 - 3.3.8[b] NIST SP 800-171 r2 - 3.3.8[c] NIST SP 800-171 r2 - 3.3.8[d] NIST SP 800-171 r2 - 3.3.8[e] NIST SP 800-171 r2 - 3.3.8[f] NIST SP 800-53 R4 AU-9(5)[S]{1} NIST SP 800-53 R4 AU-9(6)[S]{0} NIST SP 800-53 R4 AU-9[HML]{0} NIST SP 800-53 r5 - AU-9(5) NIST SP 800-53 r5 - AU-9(6) NIST SP 800-53 r5 - AU-9a

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Banking Requirements Supplemental
Level 2 Implementation (example):	Authorized access attempts to the audit system are logged. Unauthorized access attempts to the audit system are logged. The audit trails of access to the audit system are protected from modification.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.21(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-09 (HIGH; MOD) COBIT 5 DSS05.07 HIPAA Security Rule - § 164.308(a)(5)(ii)(C) ISO/IEC 27002:2022 - 8(15) NIST SP 800-53 R4 AU-9(1)[S]{0} NIST SP 800-53 r5 - AU-9(1) PCI DSS v3.2.1 10.2.3 PCI DSS v3.2.1 10.5
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High)
Level 3 Implementation (example):	The organization implements file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added does not cause an alert), and responds to any alerts generated. Logs for external-facing technologies (e.g., wireless, firewalls, DNS) are written/stored on a log server located on the internal network.
Level 3 Authoritative Source Mapping:	HIPAA Security Rule - § 164.312(c)(2) NIST Cybersecurity Framework v1.1 - RS.AN-1 NIST SP 800-53 r5 - AU-9b PCI DSS v3.2.1 10.5.4 PCI DSS v3.2.1 10.5.5 PCI DSS v3.2.1 11.5
Level CIS Implementation Requirements	
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization employs mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across organization boundaries. The information system alerts the ISSO upon detection of unauthorized access, modification, or deletion of audit information.

Level HIX Implementation Requirements	

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

Control Reference: 09.ad Administrator and Operator Logs

Control Specification:	System administrator and system operator activities shall be logged and regularly reviewed.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA PCI DSS v3.2.1 Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The organization ensures that proper logging is enabled in order to audit administrator activities. The organization ensures system administrator logs and operator logs are reviewed on a regular basis.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.35 Banking Requirements - FFIEC IS v2016 A.6.35(c) CIS Controls v7.1 - CIS CSC v7.1 6.2 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-06 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(D) ISO/IEC 27799:2016 12.4.1 ISO/IEC 27799:2016 12.4.3 NIST Cybersecurity Framework v1.1 - PR.PT-1 NIST SP 800-171 r2 - 3.3.1[a] NIST SP 800-171 r2 - 3.3.1[b] NIST SP 800-171 r2 - 3.3.1[c] NIST SP 800-171 r2 - 3.3.1[d] NIST SP 800-171 r2 - 3.3.1[e] NIST SP 800-171 r2 - 3.3.1[f] NIST SP 800-171 r2 - 3.3.3[a] NIST SP 800-171 r2 - 3.3.3[b] NIST SP 800-171 r2 - 3.3.3[c] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.3] PCI DSS v3.2.1 10.2.2 Supplemental Requirements - SR v6.4 7b.5-0

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 2 Regulatory Factors:	Banking Requirements
Level 2 Implementation (example):	An intrusion detection system managed outside of the control of system and network administrators is used to monitor system and network administration activities for compliance.
Level 2 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.35(c) Health Industry Cybersecurity Practices - 2.L.C ISO/IEC 27799:2016 12.4.3 Legacy Inheritance Support - L.I.S.

Control Reference: 09.ae Fault Logging

Control Specification:	Faults shall be logged, analyzed, and appropriate remediation action taken.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	Faults reported by users or by system programs related to problems with information processing or communications systems are logged. Error logging is enabled if this system function is available.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-02 (HIGH; MOD) COBIT 5 DSS05.07 ISO/IEC 27799:2016 12.4.1

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500

Level 2 Regulatory Factors:	FedRAMP FISMA CA Civil Code § 1798.81.5 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 2 Implementation (example):	The organization ensures there are clear rules for handling reported faults, including review of fault logs by authorized personnel in an expeditious manner to ensure that faults have been satisfactorily resolved, and review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized. The information system: identifies potentially security-relevant error conditions; generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and reveals error messages only to authorized personnel. The information system provides automated real-time alerts when faults or errors occur.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.2 CIS Controls v7.1 - CIS CSC v7.1 18.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-05(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-11 (HIGH; MOD) COBIT 5 DSS05.07 FedRAMP - SI-11a[H] FedRAMP - SI-11a[M] FedRAMP - SI-11b[H] FedRAMP - SI-11b[M] IRS Pub 1075 - SI-11a IRS Pub 1075 - SI-11b ISO/IEC 27001:2022 - 10.2h ISO/IEC 27799:2016 12.4.1 MARS-E v2.2 - SI-11a MARS-E v2.2 - SI-11b NIST SP 800-53 R4 SC-36(1)[S]{0} NIST SP 800-53 R4 SC-7(23)[S]{0} NIST SP 800-53 R4 SI-11[HM]{0} NIST SP 800-53 r5 - SC-36(1) NIST SP 800-53 r5 - SC-7(23) NIST SP 800-53 r5 - SI-11 NY OHIP Moderate-Plus Security Baseline v5.0 - AU-5(1)[NYS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - AU-5(2)[NYS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-11[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-11[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-11a NY OHIP Moderate-Plus Security Baseline v5.0 - SI-11b
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The information system monitors system operational status using operating system or system audit logs, and verifies functions and performance of the system. Logs identify where system process failures have taken place, and provide information relative to corrective actions to be taken by the system administrator.

Control Reference: 09.af Clock Synchronization

Control Specification:	The clocks of all relevant information processing systems within the organization or security domain shall be synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	CA Civil Code § 1798.81.5
Level 1 Implementation (example):	The organization uses at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.
Level 1 Authoritative Source Mapping:	CIS Controls v7.1 - CIS CSC v7.1 6.1 NIST SP 800-171 r2 - 3.3.7[a] NIST SP 800-171 r2 - 3.3.7[b] NIST SP 800-171 r2 - 3.3.7[c]

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FISMA CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	The organization synchronizes all system clocks and times where a computer or communications device has the capability to operate a real-time clock. This clock is set to an agreed standard received from industry-accepted time sources, either Coordinated Universal Time (UTC) or International Atomic Time and is accurate to within 30 seconds. The correct interpretation of the date/time format is used to ensure that the timestamp reflects the real date/time (e.g., daylight savings). The information system's internal information system clocks synchronize daily and at system boot. The organization ensures that time data is protected according to the organization's access controls and logging controls.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AU-08(01) (HIGH; MOD) IRS Pub 1075 - SC-45 ISO/IEC 27002:2022 - 8(17) ISO/IEC 27799:2016 12.4.4 NIST SP 800-53 R4 AU-8(1)[HM]{0} NIST SP 800-53 R4 AU-8(2)[S]{0} NIST SP 800-53 R4 AU-8[HML]{1} NIST SP 800-53 r5 - AU-8 NIST SP 800-53 r5 - SC-45 PCI DSS v3.2.1 10.4 PCI DSS v3.2.1 10.4.1 PCI DSS v3.2.1 10.4.2 PCI DSS v3.2.1 10.4.3

Level CIS Implementation Requirements

Level CMS Implementation Requirements

Level CMS Implementation (example):	The information system uses internal system clocks to generate time stamps for audit records, and records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and are accurate within 100 milliseconds. The information system compares the internal information system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi and synchronizes the internal system clocks to the authoritative time source when the time difference is greater than 100 milliseconds.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server. The information system compares the internal information system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi and synchronizes the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

Level NYDOH Implementation Requirements

Level NYDOH Implementation (example):	The information system compares the internal information system clocks no less often than daily and at system boot with one or more of the following federally maintained NTP stratum-1 servers: NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi); U.S. Naval Observatory Stratum-1 NTP Servers (http://tycho.usno.navy.mil/ntp.html); and CMS designated internal NTP time servers providing an NTP Stratum-2 service to the above servers.

Control Category: 10.0 - Information Systems Acquisition, Development, and Maintenance

Objective Name: 10.01 Security Requirements of Information Systems

Control Objective:	To ensure that security is an integral part of information systems.

Control Reference: 10.a Security Requirements Analysis and Specification

Control Specification:	Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems shall specify the requirements for security controls.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Specifications for the security control requirements include security controls to be incorporated in the information system, and supplemented by manual controls as needed. Further, security control requirements are considered when evaluating software packages, either developed or purchased.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) ISO/IEC 27799:2016 14.1.1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 2 Regulatory Factors:	Banking Requirements PCI DSS v3.2.1 Supplemental Requirements GDPR High Low Moderate Supplemental

Level 2 Implementation (example):	The organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with system and information integrity requirements of system and information integrity requirements/controls. The organization facilitates the implementation of system and information integrity requirements/controls. Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC8.1 Banking Requirements - FFIEC IS v2016 A.6.27 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-03 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-04(09) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) EU GDPR Article 25(1) FedRAMP - SA-3a[H] FedRAMP - SA-3a[L] FedRAMP - SA-3a[M] FedRAMP - SA-3b[H] FedRAMP - SA-3b[L] FedRAMP - SA-3b[M] FedRAMP - SA-3d[H] FedRAMP - SA-3d[L] FedRAMP - SA-3d[M] FedRAMP - SA-4(9)[H] FedRAMP - SA-4(9)[M] FedRAMP - SA-8[H] FedRAMP - SA-8[M] Health Industry Cybersecurity Practices - 5.S.B HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(8) HIPAA Security Rule - § 164.316(a) HIPAA Security Rule - § 164.316(b)(1)(i) HITRUST IRS Pub 1075 - IA-5(5) IRS Pub 1075 - SA-4(9) ISO/IEC 27002:2022 - 5(20) ISO/IEC 27002:2022 - 5(8) ISO/IEC 27002:2022 - 8(14) ISO/IEC 27002:2022 - 8(25) ISO/IEC 27002:2022 - 8(27) ISO/IEC 27002:2022 - 8(29) ISO/IEC 27799:2016 14.1.1 ISO/IEC 27799:2016 14.2.1 ISO/IEC 27799:2016 14.2.5 ISO/IEC 27799:2016 14.2.6 ISO/IEC 27799:2016 14.2.8 ISO/IEC 27799:2016 17.2.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - SA-3b MARS-E v2.2 - SA-3d MARS-E v2.2 - SA-4(9) MARS-E v2.2 - SA-8 NIST Cybersecurity Framework v1.1 - PR.IP-2 NIST Cybersecurity Framework v1.1 - RS.AN-4 NIST SP 800-171 r2 - 3.13.2[a] NIST SP 800-171 r2 - 3.13.2[b] NIST SP 800-171 r2 - 3.13.2[c] NIST SP 800-171 r2 - 3.13.2[d]

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-171 r2 - 3.13.2[e] NIST SP 800-171 r2 - 3.13.2[f] NIST SP 800-53 R4 PL-8(2)[S]{1} NIST SP 800-53 R4 SA-11(3)a[S]{2} NIST SP 800-53 R4 SA-11(3)b[S]{0} NIST SP 800-53 R4 SA-12(1)[S]{0} NIST SP 800-53 R4 SA-15(5)[S]{0} NIST SP 800-53 R4 SA-15(6)[S]{0} NIST SP 800-53 R4 SA-18(1)[S]{1} NIST SP 800-53 R4 SA-18[S]{0} NIST SP 800-53 R4 SA-3a[HML]{0} NIST SP 800-53 R4 SA-3b[HML]{0} NIST SP 800-53 R4 SA-3d[HML]{0} NIST SP 800-53 R4 SA-4(5)a[S]{1} NIST SP 800-53 R4 SA-4(6)b[S]{0} NIST SP 800-53 R4 SA-4(9)[HM]{0} NIST SP 800-53 R4 SA-8[HM]{0} NIST SP 800-53 R4 SA-9(1)b[S]{0} NIST SP 800-53 R4 SC-38[S]{0} NIST SP 800-53 R4 SI-13(5)[S]{0} NIST SP 800-53 r5 - PL-8(2) NIST SP 800-53 r5 - SA-11(3)a NIST SP 800-53 r5 - SA-11(3)b NIST SP 800-53 r5 - SA-15(5) NIST SP 800-53 r5 - SA-15(6) NIST SP 800-53 r5 - SA-15(7)d NIST SP 800-53 r5 - SA-23 NIST SP 800-53 r5 - SA-3a NIST SP 800-53 r5 - SA-3b NIST SP 800-53 r5 - SA-3d NIST SP 800-53 r5 - SA-4(5)a NIST SP 800-53 r5 - SA-4(6)b NIST SP 800-53 r5 - SA-4(9) NIST SP 800-53 r5 - SA-8 NIST SP 800-53 r5 - SA-8(1) NIST SP 800-53 r5 - SA-8(10) NIST SP 800-53 r5 - SA-8(11) NIST SP 800-53 r5 - SA-8(12) NIST SP 800-53 r5 - SA-8(13) NIST SP 800-53 r5 - SA-8(14) NIST SP 800-53 r5 - SA-8(15) NIST SP 800-53 r5 - SA-8(16) NIST SP 800-53 r5 - SA-8(17) NIST SP 800-53 r5 - SA-8(18) NIST SP 800-53 r5 - SA-8(19) NIST SP 800-53 r5 - SA-8(2) NIST SP 800-53 r5 - SA-8(20) NIST SP 800-53 r5 - SA-8(21) NIST SP 800-53 r5 - SA-8(22) NIST SP 800-53 r5 - SA-8(23) NIST SP 800-53 r5 - SA-8(24) NIST SP 800-53 r5 - SA-8(25) NIST SP 800-53 r5 - SA-8(26) NIST SP 800-53 r5 - SA-8(27) NIST SP 800-53 r5 - SA-8(28) NIST SP 800-53 r5 - SA-8(29) NIST SP 800-53 r5 - SA-8(3) NIST SP 800-53 r5 - SA-8(30) NIST SP 800-53 r5 - SA-8(31) NIST SP 800-53 r5 - SA-8(32)

Level 2 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - SA-8(4) NIST SP 800-53 r5 - SA-8(5) NIST SP 800-53 r5 - SA-8(6) NIST SP 800-53 r5 - SA-8(7) NIST SP 800-53 r5 - SA-8(8) NIST SP 800-53 r5 - SA-8(9) NIST SP 800-53 r5 - SA-9(1)b NIST SP 800-53 r5 - SC-38 NIST SP 800-53 r5 - SI-13(5) NIST SP 800-53 r5 - SR-3a NIST SP 800-53 r5 - SR-3b NIST SP 800-53 r5 - SR-5 NIST SP 800-53 r5 - SR-5(1) NIST SP 800-53 r5 - SR-9 NIST SP 800-53 r5 - SR-9(1) NY OHIP Moderate-Plus Security Baseline v5.0 - SA-4(9) PCI DSS v3.2.1 6.3 Supplemental Requirements - SR v6.4 29b.1-0 Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(d) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(f)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 3 Regulatory Factors:	FedRAMP FISMA CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	The organization develops enterprise architecture with consideration for information security, privacy, the resulting risk to organizational operations, the resulting risk to organizational assets, the resulting risk to individuals, and the resulting risk to other organizations. The organization has developed an information security architecture for the information system that describes: the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; how the information security architecture is integrated into and supports the enterprise architecture; and any information security assumptions about, and dependencies on, external services.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC5.2 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AR-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-04(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-04(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-15 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-17 (HIGH) EU GDPR Article 25(1) FedRAMP - PL-8a1[H] FedRAMP - PL-8a1[M] FedRAMP - PL-8a2[H] FedRAMP - PL-8a2[M] FedRAMP - PL-8a3[H] FedRAMP - PL-8a3[M] FedRAMP - PL-8c[H] FedRAMP - PL-8c[M] FedRAMP - SA-4(1)[H] FedRAMP - SA-4(1)[M] FedRAMP - SA-9(1)a[H] FedRAMP - SA-9(1)a[M] Health Industry Cybersecurity Practices - 9.L.C HIPAA Privacy Rule - 164.504(e)(1)(i) HIPAA Privacy Rule - 164.504(e)(5) HIPAA Security Rule - § 164.308(b)(3) HIPAA Security Rule - § 164.314(a)(1) IRS Pub 1075 - PL-8a1 IRS Pub 1075 - PL-8a2 IRS Pub 1075 - PL-8a3 IRS Pub 1075 - PL-8a4 IRS Pub 1075 - PM-7 IRS Pub 1075 - SA-4(1) IRS Pub 1075 - SA-9(1)a ISO/IEC 27002:2022 - 5(20) ISO/IEC 27002:2022 - 8(26) MARS-E v2.2 - PL-8a1 MARS-E v2.2 - PL-8a2 MARS-E v2.2 - PL-8a3 MARS-E v2.2 - PM-7 MARS-E v2.2 - SA-4(1) MARS-E v2.2 - SA-9(1) NIST Cybersecurity Framework v1.1 - ID.AM-5 NIST SP 800-53 R4 PL-8(1)b[S]{0} NIST SP 800-53 R4 PL-8a[HM]{1} NIST SP 800-53 R4 PL-8a[HM]{3} NIST SP 800-53 R4 PL-8c[HM]{0} NIST SP 800-53 R4 PM-7[HML]{0} NIST SP 800-53 R4 SA-12(2)[S]{0} NIST SP 800-53 R4 SA-17(1)[S]{0} NIST SP 800-53 R4 SA-20[S]{1} NIST SP 800-53 R4 SA-4(1)[HM]{0} NIST SP 800-53 R4 SA-4(2)[HM]{0} NIST SP 800-53 R4 SA-9(1)a[S]{0} NIST SP 800-53 R4 SI-12[HML]{3} NIST SP 800-53 r5 - IA-5(16) NIST SP 800-53 r5 - PL-7a NIST SP 800-53 r5 - PL-7b

Level 3 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - PL-8(1)b NIST SP 800-53 r5 - PL-8a1 NIST SP 800-53 r5 - PL-8a3 NIST SP 800-53 r5 - PL-8a4 NIST SP 800-53 r5 - PL-8c NIST SP 800-53 r5 - PM-7 NIST SP 800-53 r5 - SA-17(1) NIST SP 800-53 r5 - SA-20 NIST SP 800-53 r5 - SA-4(12)a NIST SP 800-53 r5 - SA-8(8) NIST SP 800-53 r5 - SA-9(1)a NIST SP 800-53 r5 - SR-6 NIST SP 800-53 r5 - SR-6(1) NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8[IS.1a1] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8[IS.1a2] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8[IS.1a3] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8[IS.1a4] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8a1 NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8a2 NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8a3 NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8a4 NY OHIP Moderate-Plus Security Baseline v5.0 - PL-8d NY OHIP Moderate-Plus Security Baseline v5.0 - PM-7 NY OHIP Moderate-Plus Security Baseline v5.0 - SA-4(1) NY OHIP Moderate-Plus Security Baseline v5.0 - SA-9(1)a Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(a)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization manages the information system using the information security steps for SDLC, as provided in the CMS system development life cycle governance process that incorporates information security control considerations. The organization requires that contracts include the standard CMS information security and privacy contract language.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization reviews and updates the information security architecture within every 365 days or when significant changes are made to the enterprise architecture, and ensures that planned information security architecture changes are reflected in the security plan and organizational procurements and acquisitions. The organization mandates the use of information technology products on the FIPS 201-approved products list for Personal Identify Verification (PIV) capability for its organizational information systems.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Whenever information systems contain FTI, the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk. The contract for system and services acquisition contains IRS Pub 1075 Exhibit 7 (E.7) language.

Level HIX Implementation Requirements	
Level HIX Implementation (example):	Each contract and Statement of Work (SOW) that contain personally identifiable information(PII) must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b). Each contract and statement of work (SOW) that contains personally identifiable information (PII) includes a definition of security roles and responsibilities and receives approval from the system owner. Acquisition contracts include a requirement that providers of defined external information systems identify the location of information systems that receive, process, store, or transmit information.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: security functional requirements; security strength requirements; security assurance requirements; security-related documentation requirements; requirements for protecting security-related documentation; a description of the information system development environment and environment in which the system is intended to operate; and acceptance criteria. The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces; source code and hardware schematics; and high-level design documentation at sufficient detail to prove the security control implementation.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization designs network and system security capabilities to leverage, integrate, and share Indicators of Compromise (IoC). The organization reviews the development process, standards, tools, and tool options/configurations at least annually to determine if the process, standards, tools, and tool options/configurations selected and employed satisfy all applicable organization-defined security requirements.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls are reconsidered prior to purchasing the product. The organization does not use free or consumer e-mail systems for business purposes.
Level VA Directive 6500 Implementation Requirements	
Level VA Directive 6500 Implementation (example):	The organization ensures that cybersecurity and privacy solutions are implemented consistent with enterprise architecture principles and guidelines within the Veterans Affairs (VA) Architecture Framework and VA cybersecurity and privacy architectures developed or approved by the VA Chief Information Officer (CIO).

Objective Name: 10.02 Correct Processing in Applications

Control Objective:	To ensure the prevention of errors, loss, unauthorized modification or misuse of information in applications, controls shall be designed into applications, including user developed applications to ensure correct processing. These controls shall include the validation of input data, internal processing and output data.

Control Reference: 10.b Input Data Validation

Control Specification:	Data input to applications and databases shall be validated to ensure that this data is correct and appropriate.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 1 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) The Joint Commission v2016 Supplemental Requirements Supplemental
Level 1 Implementation (example):	The organization develops applications based on secure coding guidelines to prevent: common coding vulnerabilities in software development processes; injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); buffer overflow (Validate buffer boundaries and truncate input strings); insecure cryptographic storage (Prevent cryptographic flaws); insecure communications (Properly encrypt all authenticated and sensitive communications); improper error handling (Do not leak information via error messages); broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user); cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.); improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and any other input-validation vulnerability listed in the OWASP Top 10.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 18.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-10 (HIGH; MOD) EU GDPR Article 25(1) ISO/IEC 27002:2022 - 8(28) NIST SP 800-53 R4 AC-24(1)[S]{0} NIST SP 800-53 R4 SI-10(1)a[S]{0} NIST SP 800-53 R4 SI-10(3)[S]{2} NIST SP 800-53 R4 SI-10(4)[S]{2} NIST SP 800-53 R4 SI-10(5)[S]{0} NIST SP 800-53 R4 SI-3(8)[S]{1} NIST SP 800-53 R4 SI-3(9)[S]{0} NIST SP 800-53 r5 - SC-16(2) NIST SP 800-53 r5 - SC-3(4) NIST SP 800-53 r5 - SI-10(1)a NIST SP 800-53 r5 - SI-10(3) NIST SP 800-53 r5 - SI-10(4) NIST SP 800-53 r5 - SI-10(5) NIST SP 800-53 r5 - SI-3(8) PCI DSS v3.2.1 6.5 PCI DSS v3.2.1 6.5.1 PCI DSS v3.2.1 6.5.10 PCI DSS v3.2.1 6.5.2 PCI DSS v3.2.1 6.5.3 PCI DSS v3.2.1 6.5.4 PCI DSS v3.2.1 6.5.5 PCI DSS v3.2.1 6.5.6 PCI DSS v3.2.1 6.5.7 PCI DSS v3.2.1 6.5.8 PCI DSS v3.2.1 6.5.9 Supplemental Requirements - SR v6.4 29a.i-0 The Joint Commission (v2016) - TJC IM.04.01.01, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 2 Regulatory Factors:	FedRAMP 23 NYCRR 500 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 2 Implementation (example):	Applications which store, process or transmit covered information undergo automated (non-manual) application vulnerability testing with an emphasis on input validation controls at least annually by a qualified party.

	For public-facing web applications, application-level firewalls are implemented. If a public-facing application is not web-based, the organization implements a network-based firewall specific to the application type. If the traffic to the public-facing application is encrypted, the device either sits behind the encryption or is capable of decrypting the traffic prior to analysis.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(h) Banking Requirements - FFIEC IS v2016 A.6.27(e) Banking Requirements - FFIEC IS v2016 A.6.27(g) CIS Controls v7.1 - CIS CSC v7.1 18.2 CIS Controls v7.1 - CIS CSC v7.1 18.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-10 (HIGH; MOD) FedRAMP - SI-10[H] FedRAMP - SI-10[M] HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(8) HIPAA Security Rule - § 164.316(b)(2)(iii) IRS Pub 1075 - SI-10 IRS Pub 1075 - SI-4(10) MARS-E v2.2 - SI-10 NIST Cybersecurity Framework v1.1 - DE.CM-8 NIST SP 800-53 R4 SI-10(2)[S]{0} NIST SP 800-53 R4 SI-10(3)[S]{1} NIST SP 800-53 R4 SI-10(4)[S]{1} NIST SP 800-53 R4 SI-10[HM]{0} NIST SP 800-53 R4 SI-4(11)[S]{0} NIST SP 800-53 R4 SI-4(18)[S]{1} NIST SP 800-53 r5 - SI-10 NIST SP 800-53 r5 - SI-10(2) NIST SP 800-53 r5 - SI-10(3) NIST SP 800-53 r5 - SI-10(4) NIST SP 800-53 r5 - SI-10(6) NIST SP 800-53 r5 - SI-4(11) NIST SP 800-53 r5 - SI-4(18) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-10 NY OHIP Moderate-Plus Security Baseline v5.0 - SI-10[IS.1] PCI DSS v3.2.1 6.6 Supplemental Requirements - SR v6.4 29a.3-0 Supplemental Requirements - SR v6.4 29b.3-0 The Joint Commission (v2016) - TJC IM.04.01.01, EP 1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 3 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) The Joint Commission v2016 Supplemental Requirements Supplemental

Level 3 Implementation (example):	Applications that are not developed using secure coding guidelines undergo automatic or manual input validation checks during testing, and annually thereafter. Input validation checks performed on applications include: dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors: out-of-range values, invalid characters in data fields, missing or incomplete data, exceeding upper and lower data volume limits, and unauthorized or inconsistent control data; periodic review of the content of key fields or data files to confirm their validity and integrity; procedures for responding to validation errors; procedures for testing the plausibility of the input data; verifying the identity of an individual opening or updating an account; defining the responsibilities of all personnel involved in the data input process; and creating a log of the activities involved in the data input process.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CIS Controls v7.1 - CIS CSC v7.1 18.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-10 (HIGH; MOD) EU GDPR Article 25(1) NIST SP 800-53 R4 AC-24(1)[S]{0} NIST SP 800-53 R4 SI-10(1)a[S]{0} NIST SP 800-53 R4 SI-10(3)[S]{2} NIST SP 800-53 R4 SI-10(4)[S]{2} NIST SP 800-53 R4 SI-10(5)[S]{0} NIST SP 800-53 R4 SI-3(8)[S]{1} NIST SP 800-53 R4 SI-3(9)[S]{0} NIST SP 800-53 r5 - SC-16(2) NIST SP 800-53 r5 - SC-3(4) NIST SP 800-53 r5 - SI-10(1)a NIST SP 800-53 r5 - SI-10(3) NIST SP 800-53 r5 - SI-10(4) NIST SP 800-53 r5 - SI-10(5) NIST SP 800-53 r5 - SI-3(8) PCI DSS v3.2.1 6.5 PCI DSS v3.2.1 6.5.1 PCI DSS v3.2.1 6.5.10 PCI DSS v3.2.1 6.5.2 PCI DSS v3.2.1 6.5.3 PCI DSS v3.2.1 6.5.4 PCI DSS v3.2.1 6.5.5 PCI DSS v3.2.1 6.5.6 PCI DSS v3.2.1 6.5.7 PCI DSS v3.2.1 6.5.8 PCI DSS v3.2.1 6.5.9 Supplemental Requirements - SR v6.4 29a.i-0 The Joint Commission (v2016) - TJC IM.04.01.01, EP 1
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization places application firewalls in front of its critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic is blocked, and an alert generated. For applications that rely on a database, the organization uses standard hardening configuration templates. All systems that are part of critical business processes are tested.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Web-enabled application software in a data warehouse: prohibits generic meta-characters in input data; arranges to have all database queries constructed with parameterized stored procedures to prevent structured query language (SQL) injection; protects any variable used in scripts to prevent direct OS command attacks; arranges to have all comments removed for any code passed to the browser; prevents users from seeing any debugging information on the client; and undergoes a check before production deployment to ensure that all sample, test, and unused files have been removed from the production system.

Control Reference: 10.c Control of Internal Processing

Control Specification:	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 1 Regulatory Factors:	DirectTrust FedRAMP 23 NYCRR 500 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The organization: develops and documents system and information integrity policy and procedures; disseminates the system and information integrity policy and procedures to appropriate areas within the organization; and reviews and updates defined system and information integrity requirements no less than annually.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.02(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-01 (HIGH; MOD) Health Industry Cybersecurity Practices - 10.M.A HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.316(b)(1)(i)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500

Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA The Joint Commission v2016 Banking Requirements PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 2 Implementation (example):	When doing system development (e.g., applications, databases), the organization ensures that the application's design and implementation minimizes the risks of processing failures leading to a loss of integrity. Data integrity controls address: the use of add, modify, and delete functions to implement changes to data; the procedures to prevent programs running in the wrong order or running after failure of prior processing; the use of appropriate programs to recover from failures to ensure the correct processing of data; and protection against attacks using buffer overruns/overflows.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(f) 23 NYCRR 500 - 500.02(b)(4) AICPA Trust Services Criteria - AICPA 2017 CC6.8 AICPA Trust Services Criteria - AICPA 2017 CC7.1 AICPA Trust Services Criteria - AICPA 2017 CC8.1 Banking Requirements - FFIEC IS v2016 A.6.27(e) Banking Requirements - FFIEC IS v2016 A.6.29 Banking Requirements - FFIEC IS v2016 A.8.1(l) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DI-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-06 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-07(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-07(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-07(05) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-07(07) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-10 (HIGH; MOD) EU GDPR Article 25(1) FedRAMP - SI-2a[H] FedRAMP - SI-2a[L] FedRAMP - SI-2a[M] FedRAMP - SI-7(7)[H] FedRAMP - SI-7(7)[M] HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(D) HIPAA Security Rule - § 164.308(a)(5)(ii)(B) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.312(b) HIPAA Security Rule - § 164.312(c)(1) HIPAA Security Rule - § 164.312(c)(2) IRS Pub 1075 - SI-2a IRS Pub 1075 - SI-7(1) IRS Pub 1075 - SI-7(10) IRS Pub 1075 - SI-7(7)b IRS Pub 1075 - SI-7a IRS Pub 1075 - SR-11a ISO/IEC 27001:2022 - 10.2a1 ISO/IEC 27001:2022 - 10.2a2 ISO/IEC 27001:2022 - 10.2b1 ISO/IEC 27001:2022 - 10.2b2 ISO/IEC 27001:2022 - 10.2c ISO/IEC 27001:2022 - 10.2f ISO/IEC 27001:2022 - 10.2g ISO/IEC 27001:2022 - 10.2h ISO/IEC 27001:2022 - 6.1.2c1 ISO/IEC 27002:2022 - 8(29) ISO/IEC 27002:2022 - 8(8) MARS-E v2.2 - SI-2a MARS-E v2.2 - SI-7 MARS-E v2.2 - SI-7(7) NIST Cybersecurity Framework v1.1 - DE.CM-8 NIST Cybersecurity Framework v1.1 - DE.DP-4 NIST Cybersecurity Framework v1.1 - ID.RA-1 NIST Cybersecurity Framework v1.1 - PR.DS-6 NIST Cybersecurity Framework v1.1 - PR.IP-12 NIST Cybersecurity Framework v1.1 - PR.IP-3 NIST Cybersecurity Framework v1.1 - RS.AN-5

Level 2 Authoritative Source Mapping (Cont.):	NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST Cybersecurity Framework v1.1 - RS.RP-1 NIST SP 800-171 r2 - 3.14.1[a] NIST SP 800-171 r2 - 3.14.1[b] NIST SP 800-171 r2 - 3.14.1[c] NIST SP 800-171 r2 - 3.14.1[d] NIST SP 800-171 r2 - 3.14.1[e] NIST SP 800-171 r2 - 3.14.1[f] NIST SP 800-53 R4 CM-3(5)[S]{2} NIST SP 800-53 R4 SA-18(1)[S]{2} NIST SP 800-53 R4 SI-2a[HML]{0} NIST SP 800-53 R4 SI-7(12)[S]{0} NIST SP 800-53 R4 SI-7(7)[HM]{0} NIST SP 800-53 R4 SI-7[HM]{0} NIST SP 800-53 r5 - CM-3(5) NIST SP 800-53 r5 - IR-5(1) NIST SP 800-53 r5 - SI-2a NIST SP 800-53 r5 - SI-7(12) NIST SP 800-53 r5 - SI-7(7) NIST SP 800-53 r5 - SI-7a NIST SP 800-53 r5 - SR-9(1) NY OHIP Moderate-Plus Security Baseline v5.0 - RA-5c NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2a NY OHIP Moderate-Plus Security Baseline v5.0 - SI-7(7) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-7(7)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-7[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-7b NY OHIP Moderate-Plus Security Baseline v5.0 - SR-11a PCI DSS v3.2.1 6.6 The Joint Commission (v2016) - TJC IM.04.01.01, EP 1 Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(h) Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(o)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs automated tools that provide notification to designated individuals (defined in the applicable security plan) upon discovering discrepancies during integrity verification. The information system automatically implements security safeguards (defined in the applicable security plan) when integrity violations are discovered and automated tools provide notification upon the discovery of discrepancies during integrity verification.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system fails to a known secure state for all failures preserving the maximum amount of state information in failure. The information system verifies the correct operation of system security functions upon system startup and restart, upon command by a user with appropriate privilege, periodically on a monthly basis, provide notification of failed automated security tests, notify system administration when anomalies are discovered, and shut down, restart or perform some other defined alternative action (defined in the applicable security plan) when anomalies are discovered. The information system automatically shuts down, restarts, or implements organization-defined security safeguards when integrity violations are discovered.

Level Providers Implementation Requirements	
Level Providers Implementation (example):	The organization's systems processing personal health information: ensures that each subject of care can be uniquely identified within the system; and are capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

Level HIPAA Implementation Requirements	

Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization incorporates domain name system (DNS) blackholing into its incident detection and response procedures, including: generating alerts to security personnel on queries to resolve blackholed domains; ensuring blackholing can be done quickly, as part of incident containment and prevention; and integrating with threat intelligence and other threat indicator sources to pre-emptively blackhole domains.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization tracks processing purposes of PII using automated mechanisms.

Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization use an incident response orchestration tool to execute established incident response playbooks.

Control Reference: 10.d Message Integrity

Control Specification:	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and controls implemented.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA The Joint Commission v2016 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Moderate Supplemental
Level 1 Implementation (example):	The information system provides mechanisms to protect the authenticity of communications sessions.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-23 (HIGH; MOD) FedRAMP - SC-23[H] FedRAMP - SC-23[M] IRS Pub 1075 - SC-23 ISO/IEC 27799:2016 10.1.1 MARS-E v2.2 - SC-23 NIST Cybersecurity Framework v1.1 - PR.AC-7 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST SP 800-171 r2 - 3.13.15[a] NIST SP 800-53 R4 AC-12(1)b[S]{0} NIST SP 800-53 R4 SC-15(4)[S]{0} NIST SP 800-53 R4 SC-23(1)[S]{0} NIST SP 800-53 R4 SC-23(3)[S]{0} NIST SP 800-53 R4 SC-23[HM]{0} NIST SP 800-53 r5 - SC-15(4) NIST SP 800-53 r5 - SC-23 NIST SP 800-53 r5 - SC-23(1) NIST SP 800-53 r5 - SC-23(3) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-23 NY OHIP Moderate-Plus Security Baseline v5.0 - SC-23[IS.1] The Joint Commission (v2016) - TJC IM.02.01.03, EP 6
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA The Joint Commission v2016 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	Cryptographic controls are implemented to ensure message authentication and integrity for covered information applications using a secure HMAC algorithm (e.g., SHA-2 or greater).
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-08 (HIGH; MOD) HIPAA Security Rule - § 164.312(e)(2)(i) ISO/IEC 27799:2016 10.1.1 OCR Guidance for Unsecured PHI (1)(ii) The Joint Commission (v2016) - TJC IM.02.01.03, EP 6
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The information system invalidates session identifiers upon user logout or other session termination.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization uniquely identifies and authenticates agency-defined system services and applications before establishing communications with devices, users, or other services or applications.

	The information system generates a unique session identifier for each session with organization-defined randomness requirements and recognizes only session identifiers that are system-generated.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	Cryptographic controls are implemented to ensure message authentication and integrity of emails. The organization implements a federated Single Sign On (SSO) solution for the authentication of all users.

Control Reference: 10.e Output Data Validation

Control Specification:	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 1 Regulatory Factors:	The Joint Commission v2016 Supplemental
Level 1 Implementation (example):	When doing system development (e.g., applications, databases), output validation: is manually or automatically performed; includes plausibility checks to test whether the output data is reasonable; includes reconciliation control counts to ensure processing of all data; includes providing sufficient information for a reader (e.g., to ensure that the client/customer they are serving matches the information retrieved, or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information); includes procedures for responding to output validation tests; includes defining the responsibilities of all personnel involved in the data output process; includes creating an automated log of activities in the data output validation process.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.03(i) EU GDPR Article 25(1) ISO/IEC 27799:2016 14.2.5 NIST SP 800-53 R4 PE-5(2)b[S]{1} NIST SP 800-53 R4 SI-15[S]{0} NIST SP 800-53 r5 - SI-15 The Joint Commission (v2016) - TJC IM.04.01.01, EP 1
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500

Level 2 Regulatory Factors:	Supplemental
Level 2 Implementation (example):	The organization uses automated output validation checks.
Level 2 Authoritative Source Mapping:	ISO/IEC 27799:2016 14.2.5 NIST SP 800-53 R4 PE-5(2)b[S]{2}

Objective Name: 10.03 Cryptographic Controls

Control Objective:	To protect the confidentiality, authenticity and integrity of information by cryptographic means. A policy shall be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

Control Reference: 10.f Policy on the Use of Cryptographic Controls

Control Specification:	A policy on the use of cryptographic controls for protection of information shall be developed, implemented, and supported by formal procedures.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust The Joint Commission v2016 Texas Medical Records Privacy Act State of Nevada Security and Privacy of Personal Information
Level 1 Implementation (example):	Encryption is used to protect covered and/or confidential information transported by mobile or removable media and across communication lines. Encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.15(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC6.7 Banking Requirements - FFIEC IS v2016 A.6.30 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-13 (HIGH; MOD) Health Industry Cybersecurity Practices - 1.M.C Health Industry Cybersecurity Practices - 4.M.C Health Industry Cybersecurity Practices - 4.S.A Health Industry Cybersecurity Practices - 7.M.C Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B HIPAA Security Rule - § 164.312(a)(2)(iv) HIPAA Security Rule - § 164.312(e)(1) HIPAA Security Rule - § 164.312(e)(2)(ii) ISO/IEC 27799:2016 10.1.1 NIST Cybersecurity Framework v1.1 - PR.PT-2 NIST Cybersecurity Framework v1.1 - PR.PT-4 OCR Guidance for Unsecured PHI (1) Ontario Personal Health Information Protection Act - 13(1) State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.215.2a The Joint Commission (v2016) - TJC IM.02.01.03, EP 2
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Banking Requirements
Level 2 Implementation (example):	When implementing the organization’s cryptographic policy and procedures, the regulations and national restrictions that apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information are adhered to.
Level 2 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.30 COBIT 5 DS5.8 COBIT 5 DSS05.03 ISO/IEC 27002:2022 - 8(24) ISO/IEC 27799:2016 10.1.1

Level PCI Implementation Requirements	
Level PCI Implementation (example):	When being assessed as a service provider, the organization maintains a documented description of the cryptographic architecture that includes: details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date; description of the key usage for each key; and inventory of any hardware security modules (HSMs) and other secure cryptographic devices (SCDs) used for key management.

Level Title 21 CFR Part 11 Implementation Requirements	
Level Title 21 CFR Part 11 Implementation (example):	The organization requires persons using electronic signatures to–prior to or at the time of such use–certify that the electronic signatures in their system–used on or after August 20, 1997–are intended to be the legally binding equivalent of traditional handwritten signatures. Such certification is required to be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. The organization also requires persons using electronic signatures to, upon request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signers hand-written signature.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	If encryption is used as an access control mechanism, the organization utilizes a level of encryption that meets CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards. SEs have a process or procedure in place for confirming that devices and media have been encrypted successfully using at least one of the following, listed in preferred order: automated policy enforcement; automated inventory system; or manual record keeping.

Control Reference: 10.g Key Management

Control Specification:	Key management shall be in place to support the organization’s use of cryptographic techniques.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	The Joint Commission v2016 Texas Medical Records Privacy Act State of Nevada Security and Privacy of Personal Information
Level 1 Implementation (example):	All cryptographic keys are protected against modification, loss, and destruction. Secret/private keys, including split-keys, are protected against unauthorized disclosure. Equipment used to generate, store, and archive keys is physically protected.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 CC6.1 Banking Requirements - FFIEC IS v2016 A.6.30 ISO/IEC 27002:2022 - 8(24) ISO/IEC 27799:2016 10.1.2 NIST SP 800-171 r2 - 3.13.10[a] NIST SP 800-171 r2 - 3.13.10[b] The Joint Commission (v2016) - TJC IM.02.01.03, EP 6
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA The Joint Commission v2016 PCI DSS v3.2.1 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information High Moderate Supplemental
Level 2 Implementation (example):	Encryption keys are not stored in the cloud (i.e., at the cloud provider in question). Encryption keys are maintained by the cloud consumer or trusted key management provider. Key management and key usage is separated. The organization's key management system is consistent with federal or industry-recognized guidelines and best practices relating to: verifying user identity prior to generating new certificates or keys; generating keys for different cryptographic systems and different applications; generating and obtaining public key certificates; distributing keys to intended users, including how keys are activated when received; storing keys in the fewest possible locations, including how authorized users obtain access to keys; changing or updating keys including rules on when keys are changed and how this will be done as deemed necessary and recommended by the associated application; and at least annually; revoking keys including how keys are withdrawn or deactivated (e.g., when keys have been compromised or suspected to have been compromised or when a user leaves an organization, in which case keys are also archived); recovering keys that are lost or corrupted as part of business continuity management (e.g., for recovery of encrypted information); archiving keys (e.g., for information archived or backed up); destroying keys; and logging and auditing of key management related activities. The organization securely manages secret and private keys, including the authenticity of public keys using public key certificates issued by a trusted Certification Authority (CA) that is a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC6.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-12 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-12(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SC-17 (HIGH; MOD) COBIT 5 DS5.8 COBIT 5 DSS05.03 FedRAMP - SC-12(1)[H] FedRAMP - SC-12[H] FedRAMP - SC-12[L] FedRAMP - SC-12[M] IRS Pub 1075 - SC-12 IRS Pub 1075 - SC-23(5) ISO/IEC 27799:2016 10.1.2 MARS-E v2.2 - SC-12 NIST Cybersecurity Framework v1.1 - PR.DS-2 NIST Cybersecurity Framework v1.1 - RC.RP-1 NIST SP 800-53 R4 SC-12(1)[H]{0} NIST SP 800-53 R4 SC-17[HM]{0} NIST SP 800-53 R4 SC-23(5)[S]{0} NIST SP 800-53 r5 - SA-9(6) NIST SP 800-53 r5 - SC-12 NIST SP 800-53 r5 - SC-12(1) NIST SP 800-53 r5 - SC-12(6) NIST SP 800-53 r5 - SC-17a NIST SP 800-53 r5 - SC-23(5) NIST SP 800-53 r5 - SC-28(3) NY OHIP Moderate-Plus Security Baseline v5.0 - SC-12 PCI DSS v3.2.1 3.5 PCI DSS v3.2.1 3.5.2 PCI DSS v3.2.1 3.5.4 PCI DSS v3.2.1 3.5.8 PCI DSS v3.2.1 3.6 PCI DSS v3.2.1 3.6.1 PCI DSS v3.2.1 3.6.2 PCI DSS v3.2.1 3.6.3 PCI DSS v3.2.1 3.6.4 PCI DSS v3.2.1 3.6.5 PCI DSS v3.2.1 3.6.7 PCI DSS v3.2.1 8.2.2

Level CMS Implementation Requirements

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The organization produces, controls, and distributes asymmetric cryptographic keys using NSA-approved key management technology and processes, approved PKI Class 3 certificates or prepositioned keying material, or approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key. The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation (example):	The organization issues public key certificates under an organization-defined certificate authority or obtains public key certificates from an approved service provider and includes only approved trust anchors in trust stores or certificate stores managed by the organization.

	The organization maintains exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization stores secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key; within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device); and as at least two full-length key components or key shares, in accordance with an industry-accepted method.

Objective Name: 10.04 Security of System Files

Control Objective:	To ensure the security of system files, access to system files and program source code shall be controlled, and IT projects and support activities conducted in a secure manner.

Control Reference: 10.h Control of Operational Software

Control Specification:	There shall be procedures in place to control the installation of software on operational systems.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	CA Civil Code § 1798.81.5 Supplemental Requirements High Supplemental
Level 1 Implementation (example):	Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions. The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse. The organization is required to deploy application allow listing technology that allows systems to run software only if it is authorized to execute (allow listed) and prevents execution of all other software on the system in accordance with the allow list and rules authorizing the terms and conditions of software program usage.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(a) AICPA Trust Services Criteria - AICPA 2017 CC8.1 CIS Controls v7.1 - CIS CSC v7.1 2.1 CIS Controls v7.1 - CIS CSC v7.1 2.7 CIS Controls v7.1 - CIS CSC v7.1 7.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07(05) (HIGH) Health Industry Cybersecurity Practices - 1.S.A Health Industry Cybersecurity Practices - 2.L.E Health Industry Cybersecurity Practices - 7.M.D Health Industry Cybersecurity Practices - 9.M.B IRS Pub 1075 - 2.B.7.3(1) ISO/IEC 27799:2016 12.5.1 NIST Cybersecurity Framework v1.1 - PR.IP-1 NIST SP 800-171 r2 - 3.4.8[a] NIST SP 800-171 r2 - 3.4.8[b] NIST SP 800-171 r2 - 3.4.8[c] NIST SP 800-53 R4 AC-4(5)[S]{2} NIST SP 800-53 R4 SC-18(4)[S]{0} NIST SP 800-53 R4 SI-7(14)[H]{0} NIST SP 800-53 r5 - AC-4(5) NIST SP 800-53 r5 - CM-7(7) NIST SP 800-53 r5 - SC-18(4) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-2a NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(2)b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(5)[IS.1] PCI DSS v3.2.1 2.2.4 Supplemental Requirements - SR v6.4 6.3-1 Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(l)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500 Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? No
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements High Moderate Supplemental
Level 2 Implementation (example):	The updating of operational software, applications, and program libraries is performed by authorized administrators. Operational systems only hold approved programs or executable code (i.e., no development code or compilers). Any decision to upgrade to a new release takes into account the business requirements for the change, the security impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version), and privacy impacts of the release.

	If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization shows evidence of a formal migration plan approved by management to replace the system or system components.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(a) Banking Requirements - FFIEC IS v2016 A.6.17 CIS Controls v7.1 - CIS CSC v7.1 18.3 CIS Controls v7.1 - CIS CSC v7.1 9.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-04 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07(05) (HIGH) FedRAMP - CM-3e[H] FedRAMP - CM-3e[M] FedRAMP - CM-7(2)[H] FedRAMP - CM-7(2)[M] Health Industry Cybersecurity Practices - 7.M.D HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(5)(ii)(B) HIPAA Security Rule - § 164.310(a)(1) HIPAA Security Rule - § 164.310(a)(2)(ii) HIPAA Security Rule - § 164.310(a)(2)(iii) HIPAA Security Rule - § 164.312(c)(1) ISO/IEC 27799:2016 12.5.1 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - CM-2(3) MARS-E v2.2 - SA-22a NIST Cybersecurity Framework v1.1 - DE.CM-2 NIST Cybersecurity Framework v1.1 - PR.DS-7 NIST SP 800-53 R4 CM-2(3)[HM]{0} NIST SP 800-53 R4 CM-7(2)[HM]{0} NIST SP 800-53 R4 CM-7(4)[M]{0} NIST SP 800-53 R4 SA-10(5)[S]{1} NIST SP 800-53 R4 SA-22(1)[S]{2} NIST SP 800-53 R4 SA-22a[S]{0} NIST SP 800-53 r5 - CM-2(3) NIST SP 800-53 r5 - CM-7(2) NIST SP 800-53 r5 - CM-7(4) NIST SP 800-53 r5 - SA-10(5) NIST SP 800-53 r5 - SA-22a NIST SP 800-53 r5 - SA-22b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(2)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11(5)b NY OHIP Moderate-Plus Security Baseline v5.0 - SA-22[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SA-22[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2[PHI.2]
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization is required to uninstall or disable unnecessary browser and email client plugins and/or add-on applications that are not absolutely necessary for the functionality of the application. Each plugin utilizes an application/URL allow listing and only allows the use of the application for pre-approved domains. The organization ensures that only authorized scripting languages are able to run in all web browsers and email clients.

Level Cloud Service Providers Implementation Requirements	
Level Cloud Service Providers Implementation (example):	Cloud service providers use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications. Structured and unstructured data is available to the organization (customer) and provided to them upon request in an industry-standard format (e.g., .doc, .xls, pdf, logs, and flat files).
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization responds to unauthorized changes to information system and components by alerting responsible actors (e.g., person, organization), restoring to the approved configuration, and halting system processing as warranted.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization replaces system components when support for the components is no longer available from the developer, vendor, or manufacturer, or provides alternative sources for continued support for unsupported components through extended security support agreement(s) that include security software patches and firmware updates from an external source(s) for each unsupported component.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization takes the following actions when unauthorized components and/or provisioned configurations are detected: disable access to the identified component; disable the identified component's network access; isolate the identified component; and notify the responsible actor (i.e., person/organization-defined in security plan). The information system prohibits user installation of software without explicit privileged status.

Control Reference: 10.i Protection of System Test Data

Control Specification:	Test data shall be selected carefully, and protected and controlled in non-production environments.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Community Supplemental Requirements 002 Supplemental
Level 1 Implementation (example):	The use of operational databases containing covered and/or confidential information for non-production (e.g., testing) purposes is avoided; however, if covered and/or confidential information is used for testing purposes, all sensitive details and content is removed or modified beyond recognition (i.e., de-identified) before use.

Level 1 Authoritative Source Mapping:	Community Supplemental Requirements 002 - CSR002 v2018 12.2-0-0 Health Industry Cybersecurity Practices - 4.M.C HIPAA Privacy Rule - 164.502(d)(1) ISO/IEC 27002:2022 - 8(33) ISO/IEC 27799:2016 14.3.1 MARS-E v2.2 - SA-11f1 MARS-E v2.2 - SA-11f3 NIST SP 800-53 R4 SA-15(9)[S]{0} NIST SP 800-53 r5 - SA-3(2)b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1b] PCI DSS v3.2.1 6.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No Is the system(s) accessible from the Internet? Yes Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Community Supplemental Requirements 002 CA Civil Code § 1798.81.5
Level 2 Implementation (example):	The organization protects operational data when used for testing purposes by applying the same access control procedures to test application systems as apply to operational application systems, requiring formal management authorization for instances where operational information is copied to a non-production application system, and erasing operational information and test accounts from a test application system immediately after the testing is complete. The organization protects operational data when used for testing purposes by applying the same security controls to non-production (test) environments as production environments, documenting all instances where covered information is used in non-production environments, and logging the copying, use, and erasure of operational information to provide an audit trail.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Community Supplemental Requirements 002 - CSR002 v2018 12.1-0-0 Community Supplemental Requirements 002 - CSR002 v2018 12.3-0-0 ISO/IEC 27002:2022 - 8(33) ISO/IEC 27799:2016 14.3.1 NIST SP 800-53 r5 - SA-3(2)a NIST SP 800-53 r5 - SA-3(2)b NY OHIP Moderate-Plus Security Baseline v5.0 - SA-3(2)b

Level FTI Custodians Implementation Requirements

Level NYDOH Implementation Requirements

Level NYDOH Implementation (example):	If production data is used for testing: it is only when a business case is documented and approved, in writing, by the information owner; all security measures, including but not limited to access controls, system configurations, and logging requirements for the production data are applied to the test environment; and the data is deleted as soon as the testing is completed; or sensitive data is masked or overwritten with fictional information.

Control Reference: 10.j Access Control to Program Source Code	
Control Specification:	Access to program source code shall be restricted.
Factor Type:	System
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Supplemental
Level 1 Implementation (example):	Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) are strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.03(i) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(4)(ii)(C) ISO/IEC 27002:2022 - 8(4) ISO/IEC 27799:2016 9.4.5 NIST SP 800-53 R4 AC-3(5)[S]{1} NIST SP 800-53 R4 SA-10(6)[S]{1} NIST SP 800-53 R4 SA-15(2)[S]{0} NIST SP 800-53 r5 - AC-3(5) NIST SP 800-53 r5 - CM-3(8) NIST SP 800-53 r5 - SA-10(6)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	FedRAMP Supplemental
Level 2 Implementation (example):	Program source code is stored in a central location, specifically in program source libraries. The following requirements are implemented to control access to such program source libraries in order to reduce the potential for corruption of computer programs: program source libraries are not held in operational systems; the program source code and the program source libraries are managed according to established procedures; access to program source libraries is strictly limited to that which is needed to perform a job function; the updating of program source libraries and associated items, and the issuing of program sources to programmers is only performed after appropriate authorization has been received; program listings are held in a secure environment; an audit log is maintained of all accesses to program source libraries; and maintenance and copying of program source libraries is subject to strict change control procedures.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AC-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05 (HIGH; MOD) ISO/IEC 27799:2016 9.4.5 NIST SP 800-53 R4 AC-3(5)[S]{2} NIST SP 800-53 R4 CM-5(6)[S]{1} NIST SP 800-53 r5 - AC-3(5) NIST SP 800-53 r5 - CM-5(6)

Objective Name: 10.05 Security In Development and Support Processes

Control Objective:	To ensure the security of application system software and information through the development process, project and support environments shall be strictly controlled.

Control Reference: 10.k Change Control Procedures

Control Specification:	The implementation of changes, including patches, service packs, and other updates and modifications, shall be controlled by the use of formal change control procedures.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust EHNAC PCI DSS v3.2.1
Level 1 Implementation (example):	The organization formally addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.11(a) Banking Requirements - FFIEC IS v2016 A.6.12 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-01 (HIGH; MOD) ISO/IEC 27799:2016 14.2.2 NIST SP 800-53 r5 - SA-10(7) PCI DSS v3.2.1 6.4

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 2 Regulatory Factors:	DirectTrust EHNAC PCI DSS v3.2.1 High Low Moderate Supplemental
Level 2 Implementation (example):	Managers responsible for application systems are responsible for the security of the project or support environment and ensuring that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment. Further, project and support environments are strictly controlled. The organization is required to manage changes to mobile device operating systems, patch levels, and/or applications through a formal change management process.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.11(a) Banking Requirements - FFIEC IS v2016 A.6.11(b) Banking Requirements - FFIEC IS v2016 A.6.11(c) Banking Requirements - FFIEC IS v2016 A.6.11(d) Banking Requirements - FFIEC IS v2016 A.6.11(e) Banking Requirements - FFIEC IS v2016 A.6.11(f) Banking Requirements - FFIEC IS v2016 A.6.11(g) Banking Requirements - FFIEC IS v2016 A.6.11(h) Banking Requirements - FFIEC IS v2016 A.6.11(i) Banking Requirements - FFIEC IS v2016 A.6.11(j) Banking Requirements - FFIEC IS v2016 A.6.11(k) Banking Requirements - FFIEC IS v2016 A.6.11(l) Banking Requirements - FFIEC IS v2016 A.6.11(m) Banking Requirements - FFIEC IS v2016 A.6.12 Banking Requirements - FFIEC IS v2016 A.6.15(d) Banking Requirements - FFIEC IS v2016 A.6.15(g) Banking Requirements - FFIEC IS v2016 A.6.15(h) Banking Requirements - FFIEC IS v2016 A.6.28(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-04(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-10 (HIGH; MOD) FedRAMP - CM-3(2)[H] FedRAMP - CM-3a[H] FedRAMP - CM-3a[M] FedRAMP - CM-9a[H] FedRAMP - CM-9a[M] FedRAMP - CM-9b[H] FedRAMP - CM-9b[M] FedRAMP - CM-9c[H] FedRAMP - CM-9c[M] FedRAMP - CM-9d[H] FedRAMP - CM-9d[M] IRS Pub 1075 - CM-3(2) IRS Pub 1075 - CM-3a IRS Pub 1075 - CM-3b IRS Pub 1075 - CM-3c IRS Pub 1075 - CM-3d IRS Pub 1075 - CM-9a IRS Pub 1075 - CM-9b IRS Pub 1075 - CM-9c IRS Pub 1075 - CM-9e IRS Pub 1075 - SA-10e ISO/IEC 27001:2022 - 8.1c ISO/IEC 27002:2022 - 8(32) ISO/IEC 27002:2022 - 8(9) ISO/IEC 27799:2016 14.2.2 ISO/IEC 27799:2016 14.2.3 ISO/IEC 27799:2016 14.2.4 ISO/IEC 27799:2016 14.2.6 ISO/IEC 27799:2016 14.2.7

Level 2 Authoritative Source Mapping (Cont.):	Legacy Inheritance Support - L.I.S. MARS-E v2.2 - CM-1a1 MARS-E v2.2 - CM-3(2) MARS-E v2.2 - CM-4(2)a MARS-E v2.2 - CM-7(1)c MARS-E v2.2 - CM-9a MARS-E v2.2 - CM-9b MARS-E v2.2 - CM-9c MARS-E v2.2 - CM-9d MARS-E v2.2 - CM-9e NIST Cybersecurity Framework v1.1 - DE.AE-1 NIST Cybersecurity Framework v1.1 - ID.RA-5 NIST Cybersecurity Framework v1.1 - ID.SC-3 NIST Cybersecurity Framework v1.1 - PR.IP-12 NIST SP 800-53 R4 CM-3(4)[S]{0} NIST SP 800-53 R4 CM-3a[HM]{0} NIST SP 800-53 R4 CM-3b[HM]{2} NIST SP 800-53 R4 CM-3g[HM]{1} NIST SP 800-53 R4 CM-4[HML]{0} NIST SP 800-53 R4 CM-9[HM]{0} NIST SP 800-53 R4 RA-5b[HML]{2} NIST SP 800-53 R4 SA-10(2)[S]{0} NIST SP 800-53 R4 SA-12(15)[S]{0} NIST SP 800-53 R4 SA-12(7)[S]{0} NIST SP 800-53 R4 SA-15(11)[S]{0} NIST SP 800-53 r5 - CM-3(4) NIST SP 800-53 r5 - CM-3a NIST SP 800-53 r5 - CM-3b NIST SP 800-53 r5 - CM-3g NIST SP 800-53 r5 - CM-4 NIST SP 800-53 r5 - CM-9a NIST SP 800-53 r5 - CM-9b NIST SP 800-53 r5 - CM-9c NIST SP 800-53 r5 - CM-9e NIST SP 800-53 r5 - RA-5b NIST SP 800-53 r5 - SA-10(2) NIST SP 800-53 r5 - SA-10(7) NIST SP 800-53 r5 - SA-15(11) NIST SP 800-53 r5 - SR-3a NIST SP 800-53 r5 - SR-4 NIST SP 800-53 r5 - SR-5(2) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-1[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-3b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-4 NY OHIP Moderate-Plus Security Baseline v5.0 - CM-4(2) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-9a NY OHIP Moderate-Plus Security Baseline v5.0 - CM-9b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-9c NY OHIP Moderate-Plus Security Baseline v5.0 - CM-9e PCI DSS v3.2.1 6.4

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	DirectTrust EHNAC FedRAMP FISMA Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 Supplemental Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 3 Implementation (example):	The organization ensures changes do not compromise existing security requirements/controls, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Change control includes: ensuring changes are submitted by authorized users; maintaining a record of agreed authorization levels; reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; identifying all software, information, database entities, and hardware that require amendment; obtaining formal approval for detailed proposals requesting changes before work commences; documenting unit, system, and user acceptance testing procedures in an environment segregated from development and production; ensuring all system components are tested and approved (operating system, utility, applications) prior to promotion to production; documenting rollback procedures for failed changes; ensuring authorized users accept changes prior to implementation based on the results on the completion of each change of testing the changes; ensuring that the system documentation set is updated and that old documentation is archived or disposed of; maintaining a version control for all software updates; maintaining an audit trail of all change requests and approvals; testing for mobile device, operating system, and application compatibility issues via a documented application validation process; and ensuring that operating documentation and user procedures are changed as necessary to remain appropriate. If a change that is not listed on the organizations approved baseline is discovered, an alert is generated and reviewed by the organization. The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. The organization reviews and updates the baseline configuration of the information system: at least once every six months; when required due to critical security patches, upgrades, emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), and major system changes/upgrades; and as an integral part of information system component installations and upgrades. Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC4.1 AICPA Trust Services Criteria - AICPA 2017 CC6.8 AICPA Trust Services Criteria - AICPA 2017 CC7.1 AICPA Trust Services Criteria - AICPA 2017 CC8.1 Banking Requirements - FFIEC IS v2016 A.6.11(c) Banking Requirements - FFIEC IS v2016 A.6.11(d) Banking Requirements - FFIEC IS v2016 A.6.11(e) Banking Requirements - FFIEC IS v2016 A.6.11(f) Banking Requirements - FFIEC IS v2016 A.6.11(g) Banking Requirements - FFIEC IS v2016 A.6.11(h) Banking Requirements - FFIEC IS v2016 A.6.11(i) Banking Requirements - FFIEC IS v2016 A.6.11(j) Banking Requirements - FFIEC IS v2016 A.6.11(m) Banking Requirements - FFIEC IS v2016 A.6.12 Banking Requirements - FFIEC IS v2016 A.6.14 Banking Requirements - FFIEC IS v2016 A.6.15(d) Banking Requirements - FFIEC IS v2016 A.6.15(g) Banking Requirements - FFIEC IS v2016 A.6.15(h) CIS Controls v7.1 - CIS CSC v7.1 11.3 CIS Controls v7.1 - CIS CSC v7.1 5.1 CIS Controls v7.1 - CIS CSC v7.1 5.2 CIS Controls v7.1 - CIS CSC v7.1 5.4 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-02(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-03(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-04(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-05(03) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06(02) (HIGH) FedRAMP - CM-2(1)a[H] FedRAMP - CM-2(1)a[M] FedRAMP - CM-2(1)c[H] FedRAMP - CM-2(1)c[M] FedRAMP - CM-2[H] FedRAMP - CM-2[L] FedRAMP - CM-2[M] FedRAMP - CM-6(1)[H] FedRAMP - CM-6(1)[M] FedRAMP - CM-6(2)[H] Health Industry Cybersecurity Practices - 2.L.A HIPAA Security Rule - § 164.308(a)(1)(ii)(D) HIPAA Security Rule - § 164.310(b) HIPAA Security Rule - § 164.316(a) IRS Pub 1075 - CM-2a IRS Pub 1075 - CM-2b1 IRS Pub 1075 - CM-2b2 IRS Pub 1075 - CM-2b3 IRS Pub 1075 - CM-3c IRS Pub 1075 - SI-7(7)a IRS Pub 1075 - SR-10

Level 3 Authoritative Source Mapping (Cont.):	ISO/IEC 27799:2016 14.2.2 ISO/IEC 27799:2016 14.2.4 MARS-E v2.2 - CM-1a1 MARS-E v2.2 - CM-6(1) MARS-E v2.2 - CM-6a MARS-E v2.2 - CM-6b MARS-E v2.2 - CM-6c MARS-E v2.2 - CM-6d NIST Cybersecurity Framework v1.1 - DE.AE-1 NIST Cybersecurity Framework v1.1 - DE.CM-7 NIST Cybersecurity Framework v1.1 - DE.DP-2 NIST Cybersecurity Framework v1.1 - PR.DS-7 NIST Cybersecurity Framework v1.1 - PR.IP-1 NIST Cybersecurity Framework v1.1 - PR.IP-3 NIST SP 800-171 r2 - 3.4.1[a] NIST SP 800-171 r2 - 3.4.1[b] NIST SP 800-171 r2 - 3.4.1[c] NIST SP 800-171 r2 - 3.4.2[a] NIST SP 800-171 r2 - 3.4.2[b] NIST SP 800-171 r2 - 3.4.5[a] NIST SP 800-171 r2 - 3.4.5[b] NIST SP 800-171 r2 - 3.4.5[c] NIST SP 800-171 r2 - 3.4.5[d] NIST SP 800-171 r2 - 3.4.5[e] NIST SP 800-171 r2 - 3.4.5[f] NIST SP 800-171 r2 - 3.4.5[g] NIST SP 800-171 r2 - 3.4.5[h] NIST SP 800-53 R4 CM-2(1)[HM]{0} NIST SP 800-53 R4 CM-2[HML]{0} NIST SP 800-53 R4 CM-3(3)[S]{0} NIST SP 800-53 R4 CM-3(5)[S]{1} NIST SP 800-53 R4 CM-3f[HM]{0} NIST SP 800-53 R4 CM-3g[HM]{2} NIST SP 800-53 R4 CM-6(1)[H]{0} NIST SP 800-53 R4 CM-6(2)[H]{1} NIST SP 800-53 R4 CM-6[HML]{0} NIST SP 800-53 R4 CM-8(6)[S]{1} NIST SP 800-53 R4 SA-10(4)[S]{1} NIST SP 800-53 R4 SA-12(7)[S]{0} NIST SP 800-53 R4 SA-15(11)[S]{0} NIST SP 800-53 R4 SA-4(5)b[S]{0} NIST SP 800-53 R4 SC-34(1)[S]{0} NIST SP 800-53 R4 SC-34[S]{0} NIST SP 800-53 R4 SI-14[S]{0} NIST SP 800-53 r5 - CM-2 NIST SP 800-53 r5 - CM-3(3) NIST SP 800-53 r5 - CM-3(5) NIST SP 800-53 r5 - CM-3f NIST SP 800-53 r5 - CM-3g NIST SP 800-53 r5 - CM-6 NIST SP 800-53 r5 - CM-6(1) NIST SP 800-53 r5 - CM-6(2) NIST SP 800-53 r5 - CM-8(6) NIST SP 800-53 r5 - SA-10(4) NIST SP 800-53 r5 - SA-15(11) NIST SP 800-53 r5 - SA-4(5)b NIST SP 800-53 r5 - SC-34 NIST SP 800-53 r5 - SC-34(1) NIST SP 800-53 r5 - SI-14 NIST SP 800-53 r5 - SR-4

Level 3 Authoritative Source Mapping (Cont.):	NIST SP 800-53 r5 - SR-5(2) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-2(2)[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-2b3 NY OHIP Moderate-Plus Security Baseline v5.0 - CM-6(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(1)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(1)[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(1)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7(2)b NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - CM-7[IS.2] PCI DSS v3.2.1 6.4 Supplemental Requirements - SR v6.4 17.9-0 Supplemental Requirements - SR v6.4 6.1-0 Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(c)

Level CIS Implementation Requirements

Level CIS Implementation (example):	The organization builds secure images for workstations, servers and other system types from their secure configuration baselines and uses these images to build all new systems it deploys. Any existing systems that must be rebuilt (e.g., due to compromise) are rebuilt from the organizations secure images. Master images, including regular updates and exceptions, are formally managed by the organization’s change management processes to ensure that only authorized changes are possible.

Level CMS Implementation Requirements

Level CMS Implementation (example):	HHS-specific minimum security configurations are used for the following Operating System (OS) and Applications: HHS approved Windows Standards; Blackberry Server; Websense. The organization uses the following CMS hierarchy for implementing security configuration guidelines when an HHS-specific minimum security configuration does not exist, and to resolve configuration conflicts among multiple security guidelines: USGCB; NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order; Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); National Security Agency (NSA) STIGs; if formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group, i.e., the Center for Internet Security (CIS), checklists. In situations where no guidance exists, coordinate with CMS for guidance. CMS collaborates within CMS and the HHS Cybersecurity Program, and other organizations through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to: (a) establish baseline configurations and communicate industry and vendor best practices; and (b) ensure deployed configurations are supported for security updates. All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation (example):	The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication must be approved and accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO).

	The information system prevents the installation of network, server, and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	All organization information systems used for receiving, processing, storing, and transmitting FTI must be hardened (securely configured) using, when available for the specific technologies used, Safeguard Computer Security Evaluation Matrices (SCSEMs) publicly available on the Office of Safeguards IRS.gov website, keyword: safeguards program. The organization requires organizational designated security and privacy representatives to be included in the configuration change management and control process.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	HHS-specific minimum security configurations are used for the following Operating System (OS) and Applications: HHS approved Windows Standards, Blackberry Server, and Websense; and for all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the organization uses the CMS hierarchy for implementing security configuration guidelines. Further determine if formal government-authored checklists do not exist, then organizations use vendor or industry group guidance, if available. The organization also ensures checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). The organization analyzes changes to an information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. Processing or storing of personally identifiable information (PII) in test environments is prohibited.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	Upon completion of a significant change, all relevant PCI DSS requirements are implemented on all new or changed systems and networks, and documentation is updated as applicable.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization requires the developer of the information system, system component, or information system service to: perform configuration management during system, component, or service development, implementation, and operation; document, manage, and control the integrity of changes to configuration items under configuration management; implement only organization-approved changes to the system, component, or service; document approved changes to the system, component, or service and the potential security impacts of such changes; and track security flaws and flaw resolution within the system, component, or service, and report findings to defined personnel or roles (defined in the applicable system security plan).

Control Reference: 10.l Outsourced Software Development

Control Specification:	Outsourced software development shall be supervised and monitored by the organization.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	Where software development is outsourced, formal contracts are in place to address: licensing arrangements; code ownership; intellectual property rights; certification of the quality and accuracy of the work; rights of access for the audit of the quality and accuracy of work; escrow arrangements; quality and security functionality requirements for the developed code; and security testing and evaluation prior to installation.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.08(a) Banking Requirements - FFIEC IS v2016 A.6.28(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-11 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SA-13 (HIGH) ISO/IEC 27799:2016 14.2.7 NIST Cybersecurity Framework v1.1 - DE.CM-4 NIST Cybersecurity Framework v1.1 - ID.BE-1
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? No
Level 2 Regulatory Factors:	FISMA Banking Requirements CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	The development of all outsourced software is supervised and monitored by the organization. Where software development is outsourced, the development process is monitored by the organization and includes monitoring of security requirements, independent security review of the outsourced environment by a certified individual, certified security training for outsourced software developers, and code reviews.
Level 2 Authoritative Source Mapping:	Banking Requirements - FFIEC IS v2016 A.6.28 Banking Requirements - FFIEC IS v2016 A.6.28(b) Banking Requirements - FFIEC IS v2016 A.6.28(d) IRS Pub 1075 - SA-11(4) ISO/IEC 27002:2022 - 8(28) ISO/IEC 27002:2022 - 8(30) ISO/IEC 27799:2016 14.2.7 NIST Cybersecurity Framework v1.1 - DE.CM-6

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization protects against supply chain threats by employing leading practices and methodologies such as, wherever possible, selecting components that have been previously reviewed by other government entities, e.g., National Information Assurance Partnership (NIAP), as part of a comprehensive, defense-in-breadth information security strategy).

Objective Name: 10.06 Technical Vulnerability Management

Control Objective:	To reduce the risks resulting from exploitation of published technical vulnerabilities, technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

Control Reference: 10.m Control of Technical Vulnerabilities

Control Specification:	Timely information about technical vulnerabilities of information systems being used shall be obtained; the organization's exposure to such vulnerabilities evaluated; and appropriate measures taken to address the associated risk.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	CA Civil Code § 1798.81.5 State of Massachusetts Data Protection Act (201 CMR 17.00) High Low Moderate Supplemental
Level 1 Implementation (example):	Once a potential technical vulnerability has been identified, the organization identifies the associated risks and the actions to be taken. Further, the organization performs the necessary actions to correct identified technical vulnerabilities in a timely manner. Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.2 or later, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.4.4 Banking Requirements - FFIEC IS v2016 A.6.13 Banking Requirements - FFIEC IS v2016 A.8.3 CIS Controls v7.1 - CIS CSC v7.1 3.6 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05 (HIGH; MOD) Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 7.L.B Health Industry Cybersecurity Practices - 7.M.A Health Industry Cybersecurity Practices - 7.M.D Health Industry Cybersecurity Practices - 7.S.A Health Industry Cybersecurity Practices - 9.L.A Health Industry Cybersecurity Practices - 9.M.A Health Industry Cybersecurity Practices - 9.M.B IRS Pub 1075 - SI-2(IRS-1) ISO/IEC 27001:2022 - 10.2b3 ISO/IEC 27799:2016 12.6.1 MARS-E v2.2 - CM-7b NIST Cybersecurity Framework v1.1 - ID.RA-1 NIST Cybersecurity Framework v1.1 - PR.DS-8 NIST Cybersecurity Framework v1.1 - PR.IP-12 NIST Cybersecurity Framework v1.1 - RS.AN-5 NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST SP 800-171 r2 - 3.11.3[a] NIST SP 800-171 r2 - 3.11.3[b] NIST SP 800-171 r2 - 3.12.2[a] NIST SP 800-171 r2 - 3.12.2[b] NIST SP 800-171 r2 - 3.12.2[c] NIST SP 800-171 r2 - 3.4.7[a] NIST SP 800-171 r2 - 3.4.7[b] NIST SP 800-171 r2 - 3.4.7[c] NIST SP 800-171 r2 - 3.4.7[d] NIST SP 800-171 r2 - 3.4.7[e] NIST SP 800-171 r2 - 3.4.7[f] NIST SP 800-171 r2 - 3.4.7[g] NIST SP 800-171 r2 - 3.4.7[h] NIST SP 800-171 r2 - 3.4.7[i] NIST SP 800-171 r2 - 3.4.7[j] NIST SP 800-171 r2 - 3.4.7[k] NIST SP 800-171 r2 - 3.4.7[l] NIST SP 800-171 r2 - 3.4.7[m] NIST SP 800-171 r2 - 3.4.7[n] NIST SP 800-171 r2 - 3.4.7[o] NIST SP 800-53 R4 CM-7a[HML]{1} NIST SP 800-53 R4 CM-7b[HML]{2} NIST SP 800-53 R4 SC-7(17)[S]{0} NIST SP 800-53 r5 - CM-7a NIST SP 800-53 r5 - CM-7b NIST SP 800-53 r5 - RA-3a1 NIST SP 800-53 r5 - SC-41 NIST SP 800-53 r5 - SC-7(17) NIST SP 800-53 r5 - SR-10 NY OHIP Moderate-Plus Security Baseline v5.0 - AC-17[IS.3a] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2(5) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2c NY OHIP Moderate-Plus Security Baseline v5.0 - SR-10 NY OHIP Moderate-Plus Security Baseline v5.0 - SR-10[IS.1] PCI DSS v3.2.1 2.2.2

Level 1 Authoritative Source Mapping (Cont.):	PCI DSS v3.2.1 2.2.3 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.04(6)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Supplemental Requirements Supplemental
Level 2 Implementation (example):	The configuration standard for all system components (workstations, databases, servers, applications, routers, switches, wireless access points) are hardened to address, to the extent practical, all known security vulnerabilities. In particular, laptops, workstations, and servers are configured so they will not auto-run content from removable media (e.g., USB tokens–thumb drives, USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares). The organization's configuration standards are consistent with industry-accepted system hardening standards (e.g., CIS, ISO, NIST, SANS). The organization defines and establishes the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required. The organization also establishes a process to identify and assign a risk ranking to newly discovered security vulnerabilities which considers the CVSS score, classification of the vendor supplied patch, and/or the classification and criticality of the affected system.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.05(b) AICPA Trust Services Criteria - AICPA 2017 CC7.1 AICPA Trust Services Criteria - AICPA 2017 CC7.4 Banking Requirements - FFIEC IS v2016 A.10.1 Banking Requirements - FFIEC IS v2016 A.10.3(c) Banking Requirements - FFIEC IS v2016 A.6.13 Banking Requirements - FFIEC IS v2016 A.6.15(c) Banking Requirements - FFIEC IS v2016 A.6.15(d) Banking Requirements - FFIEC IS v2016 A.6.15(f) Banking Requirements - FFIEC IS v2016 A.6.15(h) Banking Requirements - FFIEC IS v2016 A.6.27(d) Banking Requirements - FFIEC IS v2016 A.8.1(c) Banking Requirements - FFIEC IS v2016 A.8.3 Banking Requirements - FFIEC IS v2016 A.8.4 CIS Controls v7.1 - CIS CSC v7.1 18.11 CIS Controls v7.1 - CIS CSC v7.1 3.7 CIS Controls v7.1 - CIS CSC v7.1 5.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CM-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05 (HIGH; MOD) Health Industry Cybersecurity Practices - 2.M.A Health Industry Cybersecurity Practices - 7.M.A Health Industry Cybersecurity Practices - 7.M.D HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(8) IRS Pub 1075 - RA-5(IRS-1) ISO/IEC 27002:2022 - 8(8) ISO/IEC 27799:2016 12.6.1 NIST Cybersecurity Framework v1.1 - DE.CM-8 NIST Cybersecurity Framework v1.1 - ID.RA-1 NIST Cybersecurity Framework v1.1 - PR.DS-8 NIST Cybersecurity Framework v1.1 - PR.IP-12 NIST Cybersecurity Framework v1.1 - PR.IP-3 NIST Cybersecurity Framework v1.1 - RS.AN-5 NIST Cybersecurity Framework v1.1 - RS.MI-3 NIST SP 800-53 R4 SA-15(7)b[S]{0} NIST SP 800-53 R4 SA-15(7)c[S]{0} NIST SP 800-53 r5 - CA-2a NIST SP 800-53 r5 - SA-11(2)a NIST SP 800-53 r5 - SA-15(7)b NIST SP 800-53 r5 - SA-15(7)c NIST SP 800-53 r5 - SC-7(10)b NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2[IS.1a] PCI DSS v3.2.1 11.2 PCI DSS v3.2.1 11.2.1 PCI DSS v3.2.1 11.2.2 PCI DSS v3.2.1 11.2.3 PCI DSS v3.2.1 2.2 PCI DSS v3.2.1 6.1 PCI DSS v3.2.1 6.4.5 Supplemental Requirements - SR v6.4 2-0 Supplemental Requirements - SR v6.4 32-2 Supplemental Requirements - SR v6.4 32b-0 Veterans Affairs Cybersecurity Program Directive 6500 - b(4)(e)

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA 23 NYCRR 500 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	The organization conducts an enterprise security posture review as needed, but no less than once within every 365 days, in accordance with organizational information security procedures. The organization's vulnerability scanning tools are regularly updated with all relevant information system vulnerabilities or it updates its list of vulnerabilities based on a subscription to one or more vulnerability intelligence services to stay aware of emerging exposures.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.8.1(d) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CA-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 RA-05(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-02(01) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-02(02) (HIGH; MOD) COBIT 5 DS5.9 COBIT 5 DSS05.02 FedRAMP - CA-8(1)[H] FedRAMP - CA-8(1)[M] FedRAMP - CA-8[H] FedRAMP - CA-8[M] FedRAMP - RA-5(1)[H] FedRAMP - RA-5(1)[M] FedRAMP - RA-5(2)[H] FedRAMP - RA-5(2)[M] FedRAMP - RA-5(3)[H] FedRAMP - RA-5(3)[M] FedRAMP - RA-5(8)[H] FedRAMP - RA-5(8)[M] FedRAMP - SI-2(2)[H] FedRAMP - SI-2(2)[M] Health Industry Cybersecurity Practices - 7.L.B Health Industry Cybersecurity Practices - 7.S.A HIPAA Security Rule - § 164.308(a)(1)(ii)(D) IRS Pub 1075 - CA-8 IRS Pub 1075 - RA-5(2) IRS Pub 1075 - RA-5(5) IRS Pub 1075 - RA-5f ISO/IEC 27001:2022 - 10.2b3 MARS-E v2.2 - CA-8(1) MARS-E v2.2 - RA-5(1) MARS-E v2.2 - RA-5(3) MARS-E v2.2 - RA-5(5) MARS-E v2.2 - RA-5(8) MARS-E v2.2 - SI-2(2) NIST Cybersecurity Framework v1.1 - DE.CM-8 NIST Cybersecurity Framework v1.1 - ID.RA-1 NIST Cybersecurity Framework v1.1 - PR.IP-12 NIST SP 800-171 r2 - 3.11.2[a] NIST SP 800-171 r2 - 3.11.2[b] NIST SP 800-171 r2 - 3.11.2[c] NIST SP 800-171 r2 - 3.11.2[d] NIST SP 800-171 r2 - 3.11.2[e] NIST SP 800-53 R4 AC-4(11)[S]{0} NIST SP 800-53 R4 CA-8(1)[S]{0} NIST SP 800-53 R4 CA-8(2)[S]{0} NIST SP 800-53 R4 CA-8[H]{0} NIST SP 800-53 R4 RA-5(1)[HM]{0} NIST SP 800-53 R4 RA-5(2)[HM]{0} NIST SP 800-53 R4 RA-5(3)[S]{0} NIST SP 800-53 R4 RA-5(5)[HM]{0} NIST SP 800-53 R4 RA-5(8)[S]{0} NIST SP 800-53 R4 RA-5a[HML]{0} NIST SP 800-53 R4 SA-12(11)[S]{0}

Level 3 Authoritative Source Mapping (Cont.):	NIST SP 800-53 R4 SA-15(7)a[S]{0} NIST SP 800-53 R4 SI-2(2)[HM]{0} NIST SP 800-53 r5 - AC-4(11) NIST SP 800-53 r5 - CA-8 NIST SP 800-53 r5 - CA-8(1) NIST SP 800-53 r5 - CA-8(2) NIST SP 800-53 r5 - RA-5(2) NIST SP 800-53 r5 - RA-5(3) NIST SP 800-53 r5 - RA-5(5) NIST SP 800-53 r5 - RA-5(8) NIST SP 800-53 r5 - RA-5a NIST SP 800-53 r5 - RA-5f NIST SP 800-53 r5 - SA-11(2)c NIST SP 800-53 r5 - SA-15(7)a NIST SP 800-53 r5 - SI-2(2) NIST SP 800-53 r5 - SR-6(1) NY OHIP Moderate-Plus Security Baseline v5.0 - RA-5(5) NY OHIP Moderate-Plus Security Baseline v5.0 - RA-5f PCI DSS v3.2.1 11.3 PCI DSS v3.2.1 11.3.1 PCI DSS v3.2.1 11.3.2 PCI DSS v3.2.1 11.3.3 PCI DSS v3.2.1 11.3.4 PCI DSS v3.2.1 6.2 Veterans Affairs Cybersecurity Program Directive 6500 - a(4)(d) Veterans Affairs Cybersecurity Program Directive 6500 - c(1)(b) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(o)
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization installs the latest stable version of any security-related updates on all network devices. The organization performs periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization corrects identified information system flaws on production equipment within 10 business days and all others within 30 calendar days. A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) if a security patch is not applied to a security-based system or network.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization updates the list of information system vulnerabilities scanned prior to a new scan or when new vulnerabilities are identified and reported. The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.
Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation (example):	The organization conducts both internal and external penetration testing as needed but no less than once within every 365 days, in accordance with the organizations information security procedures. The results of such testing must be reported to management.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization ensures that multifunction Device (MFD) firmware is supported by the vendor and is kept up to date with the most current firmware available. Vulnerability assessments are performed on systems in a virtualized environment prior to system implementation and frequently thereafter.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization performs external network penetration testing and conducts an enterprise security posture review as needed but no less than once within every 365 days, in accordance with organizational information security procedures. The organization mitigates legitimate high-risk vulnerabilities within 30 days and moderate risk vulnerabilities within 90 days.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization performs quarterly internal vulnerability scans and rescans, which may be automated, manual, or a combination thereof, as needed, until all “high-risk” vulnerabilities are resolved in accordance with the organizations vulnerability rankings. Scans are performed by qualified personnel. The organization performs quarterly external vulnerability scans, external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC), rescans as needed, until passing scans are achieved, internal scans, and external scans. The organization rescans as needed, after any significant change. Scans are performed by qualified personnel. The organization implements a methodology for penetration testing that: is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115); includes coverage for the entire card data environment (CDE) perimeter and critical systems; includes testing from both inside and outside the network; includes testing to validate any segmentation and scope-reduction controls; defines application-layer penetration tests to include, at a minimum, the vulnerabilities identified in PCI DSS v3.1; defines network-layer penetration tests to include components that support network functions as well as operating systems; includes review and consideration of threats and vulnerabilities experienced in the last 12 months; and specifies retention of penetration testing results and remediation activities results.
Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation (example):	Maintain and adhere to a documented process to remediate all critical, high, and medium risk security vulnerabilities promptly.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization identifies vulnerabilities exploited during a security incident and implements security safeguards to reduce risk and vulnerability exploit exposure, including isolating or disconnecting systems. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization establishes a public reporting channel for receiving reports of vulnerabilities in the organization's systems and system components.

Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization monitors command and control (C2) traffic for indicators of an attack. The organization uses specialized vulnerability scanners to interrogate running web applications to check for vulnerabilities in the application design. Vulnerabilities identified during the scan are tracked to resolution.

Control Category: 11.0 - Information Security Incident Management

Objective Name: 11.01 Reporting Information Security Incidents and Weaknesses

Control Objective:	To ensure information security events and weaknesses associated with information systems are handled in a manner allowing timely corrective action to be taken.

Control Reference: 11.a Reporting Information Security Events

Control Specification:	Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third-party users shall be made aware of their responsibility to report any information security events as quickly as possible.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	SCIDSA State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act
Level 1 Implementation (example):	A point of contact is established for the reporting of information security events. It is ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response. The organization also maintains a list of third-party contact information (e.g., the email addresses of their information security officers), which can be used to report a security incident.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) Banking Requirements - FFIEC IS v2016 A.8.5(f) Banking Requirements - FFIEC IS v2016 A.8.5(g) CIS Controls v7.1 - CIS CSC v7.1 19.5 HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) ISO/IEC 27799:2016 16.1.1 NIST Cybersecurity Framework v1.1 - RS.CO-2 NIST Cybersecurity Framework v1.1 - RS.CO-3 NIST Cybersecurity Framework v1.1 - RS.CO-4 NY OHIP Moderate-Plus Security Baseline v5.0 - IR-6b NY OHIP Moderate-Plus Security Baseline v5.0 - RA-5[IS.4] PCI DSS v3.2.1 12.10.3

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FedRAMP FISMA HITRUST De-ID Framework 23 NYCRR 500 Banking Requirements CA Civil Code § 1798.81.5 PCI DSS v3.2.1 SCIDSA State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) State of Nevada Security and Privacy of Personal Information High Low Moderate Supplemental
Level 2 Implementation (example):	Formal information security event reporting procedures to support the corporate direction (policy) are established, set out the action to be taken on receipt of a report of an information security event, set out the treating of breach as discovered, set out the timeliness of reporting and response, set out the time required for system administrators and other personnel to report anomalous events to the incident handling team, set out the mechanisms for such reporting, and set out the kind of information that is included in the incident notification. Formal information security event reporting also includes notifying internal stakeholders (in accordance with all legal or regulatory requirements for involving them in computer incidents), notifying external stakeholders (in accordance with all legal or regulatory requirements for involving them in computer incidents), notifying the appropriate Community Emergency Response Team, and notifying law enforcement agencies (in accordance with all legal or regulatory requirements for involving them in computer incidents). Given the importance of Information Security Incident Handling, a policy is established to set the direction of management. Employees and other workforce members, including third-parties, are able to freely report security weaknesses (real and perceived) without fear of repercussion. The organization has implemented an insider threat program that includes a cross-discipline insider threat incident handling team.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(2) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 CC2.3 AICPA Trust Services Criteria - AICPA 2017 CC7.3 AICPA Trust Services Criteria - AICPA 2017 CC7.4 AICPA Trust Services Criteria - AICPA 2017 CC7.5 AICPA Trust Services Criteria - AICPA 2017 P6.5 Banking Requirements - FFIEC IS v2016 A.6.21(b) Banking Requirements - FFIEC IS v2016 A.6.31(f) Banking Requirements - FFIEC IS v2016 A.8.1(b) Banking Requirements - FFIEC IS v2016 A.8.1(j) Banking Requirements - FFIEC IS v2016 A.8.5(a) Banking Requirements - FFIEC IS v2016 A.8.5(b) Banking Requirements - FFIEC IS v2016 A.8.5(d) Banking Requirements - FFIEC IS v2016 A.8.5(e) Banking Requirements - FFIEC IS v2016 A.8.5(f) Banking Requirements - FFIEC IS v2016 A.8.5(g) CIS Controls v7.1 - CIS CSC v7.1 19.1 CIS Controls v7.1 - CIS CSC v7.1 19.2 CIS Controls v7.1 - CIS CSC v7.1 19.3 CIS Controls v7.1 - CIS CSC v7.1 19.4 CIS Controls v7.1 - CIS CSC v7.1 19.5 CIS Controls v7.1 - CIS CSC v7.1 19.6 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02 (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-12 (HIGH; MOD) COBIT 5 DS5.6 COBIT 5 DSS02.01 COBIT 5 DSS05.07 FedRAMP - IR-4(6)[H] FedRAMP - SI-4(19)[H] Health Industry Cybersecurity Practices - 10.S.A Health Industry Cybersecurity Practices - 2.S.A Health Industry Cybersecurity Practices - 6.M.C Health Industry Cybersecurity Practices - 8.S.A HIPAA Breach Notification Rule - 164.404(b) HIPAA Breach Notification Rule - 164.404(c)(1)(A) HIPAA Breach Notification Rule - 164.404(c)(1)(B) HIPAA Breach Notification Rule - 164.404(c)(1)(C) HIPAA Breach Notification Rule - 164.404(c)(1)(D) HIPAA Breach Notification Rule - 164.404(c)(1)(E) HIPAA Breach Notification Rule - 164.406(c) HIPAA Breach Notification Rule - 164.410(a)(2) HIPAA Breach Notification Rule - 164.412(a) HIPAA Breach Notification Rule - 164.412(b) HIPAA Privacy Rule - 164.504(e)(1)(ii) HIPAA Privacy Rule - 164.504(e)(2)(ii)(C) HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(1)(ii)(C) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.316(b)(2)(ii) IRS Pub 1075 - IR-4(6)

Level 2 Authoritative Source Mapping (Cont.):	IRS Pub 1075 - IR-8(1)a IRS Pub 1075 - PM-12 ISO/IEC 27002:2022 - 5(25) ISO/IEC 27002:2022 - 8(7) ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.2 ISO/IEC 27799:2016 16.1.3 ISO/IEC 27799:2016 16.1.4 ISO/IEC 27799:2016 7.2.1 ISO/IEC 27799:2016 7.2.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - PM-12 MARS-E v2.2 - PM-16 NIST Cybersecurity Framework v1.1 - DE.AE-5 NIST Cybersecurity Framework v1.1 - DE.DP-4 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST Cybersecurity Framework v1.1 - ID.SC-5 NIST Cybersecurity Framework v1.1 - PR.IP-11 NIST Cybersecurity Framework v1.1 - RC.CO-1 NIST Cybersecurity Framework v1.1 - RC.CO-2 NIST Cybersecurity Framework v1.1 - RC.CO-3 NIST Cybersecurity Framework v1.1 - RS.AN-1 NIST Cybersecurity Framework v1.1 - RS.AN-4 NIST Cybersecurity Framework v1.1 - RS.AN-5 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-2 NIST Cybersecurity Framework v1.1 - RS.CO-3 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST Cybersecurity Framework v1.1 - RS.CO-5 NIST SP 800-53 R4 AT-2(1)[S]{1} NIST SP 800-53 R4 IR-4(6)[S]{0} NIST SP 800-53 R4 IR-4(7)[S]{0} NIST SP 800-53 R4 IR-4(9)[S]{0} NIST SP 800-53 R4 IR-6(3)[S]{0} NIST SP 800-53 R4 IR-6a[HML]{0} NIST SP 800-53 R4 IR-7(2)b[S]{0} NIST SP 800-53 R4 IR-8a[HML]{2} NIST SP 800-53 R4 IR-8a[HML]{5} NIST SP 800-53 R4 PM-12[HML]{0} NIST SP 800-53 R4 SA-15(10)[S]{1} NIST SP 800-53 R4 SI-4(19)[S]{1} NIST SP 800-53 R4 SI-4a[HML]{0} NIST SP 800-53 r5 - AT-2(1) NIST SP 800-53 r5 - IR-2(3) NIST SP 800-53 r5 - IR-4(6) NIST SP 800-53 r5 - IR-4(7) NIST SP 800-53 r5 - IR-4(9) NIST SP 800-53 r5 - IR-6(3) NIST SP 800-53 r5 - IR-6a NIST SP 800-53 r5 - IR-7(2)b NIST SP 800-53 r5 - IR-8(1)a NIST SP 800-53 r5 - IR-8a2 NIST SP 800-53 r5 - IR-8a5 NIST SP 800-53 r5 - PM-12 NIST SP 800-53 r5 - SA-15(10) NIST SP 800-53 r5 - SI-4(19) NY OHIP Moderate-Plus Security Baseline v5.0 - IR-8(1)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-8(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-12 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-12[IS.1c]

Level 2 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - PM-12[IS.1e] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-16 PCI DSS v3.2.1 12.10 PCI DSS v3.2.1 12.10.1 PCI DSS v3.2.1 12.10.3 PCI DSS v3.2.1 12.10.4 PCI DSS v3.2.1 12.10.5 South Carolina Insurance Data Security Act (SCIDSA) - SCIDSA 33-99-20(H) State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(j) State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.1 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.2 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.3 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.4 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.5a State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.6 Supplemental Requirements - SR v6.4 34b.i-0 Supplemental Requirements - SR v6.4 34b.ii-0 Supplemental Requirements - SR v6.4 35-0 Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(b) Veterans Affairs Cybersecurity Program Directive 6500 - c(1)(h) Veterans Affairs Cybersecurity Program Directive 6500 - c(2)(g) Veterans Affairs Cybersecurity Program Directive 6500 - c(3)(b)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation (example):	A duress alarm is provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms reflect the high-risk situation such alarms are indicating. An information security assessment is made either on all incidents or on a sample, to further validate the effectiveness or otherwise of established controls and of the risk assessment that lead to them.
Level 3 Authoritative Source Mapping:	HIPAA Security Rule - § 164.308(a)(1)(ii)(D) HIPAA Security Rule - § 164.308(a)(6)(i) ISO/IEC 27799:2016 16.1.2 ISO/IEC 27799:2016 16.1.6 NIST Cybersecurity Framework v1.1 - PR.IP-7
Level Cloud Service Providers Implementation Requirements	
Level Cloud Service Providers Implementation (example):	Cloud service providers make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current CMS Incident Handling and Breach Notification Standard.
Level De-ID Data Environment Implementation Requirements	
Level De-ID Data Environment Implementation (example):	Organizations receiving de-identified data notify the providing organization's data custodian of any breach involving de-identified data in order to determine the appropriate response. The organization tracks visitor-related incidents and that corrective actions are taken when they occur.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	Any data incident potentially involving FTI is immediately reported to the appropriate Treasury Inspector General for the Tax Administration (TIGTA) field office and the IRS Office of Safeguards immediately, but no later than twenty-four (24) hours after identification of a possible issue involving FTI. The organization documents in a data incident report the following aspect of the incident to the extent it is known at the time: Name of organization and organization Point of Contact for resolving data incident with contact information; Date and time of the incident; Date and time the incident was discovered; How the incident was discovered; Description of the incident and the data involved, including specific data elements, if known; Potential number of FTI records involved; if unknown, provide a range if possible; Address where the incident occurred; IT involved (e.g., laptop, server, mainframe). FTI is not included in the data Incident report. Reports are sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. The organization informs the Office of Safeguards of notification activities undertaken before release to individuals impacted by a breach of FTI and of any pending media releases, including sharing the text, prior to distribution.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	In the case of a personal data breach, the controller notifies the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and liberties (freedoms) of natural persons. Such notification is provided all at once or, if in phases, without further undue delay, at least describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned, at least communicate the name and contact details of the data protection officer or other contact point where more information can be obtained, at least describe the likely consequences of the personal data breach, and at least describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where the notification to the supervisory authority is not made within 72 hours, it is accompanied by reasons for the delay. The organization, acting as a data processor, notifies the data controller without undue delay after becoming aware of a personal data breach.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization follows CMS Incident Reporting requirements for reporting incidents to oversight organizations.

Level PCI Implementation Requirements	
Level PCI Implementation (example):	The organization designates specific personnel to be available on a 24 hours, seven days a week (24/7) basis to respond to alerts.
Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation (example):	The organization ensures that workforce members do not interfere with federal or state investigations or disciplinary proceedings through willful misrepresentation or omission of facts or by the use of threats or harassment against any person. Breach disclosures are made as quickly as possible, except at the request of a law enforcement agency that determines notification will impede a criminal investigation, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation (example):	The organization notifies the superintendent of financial services for the state of New York within 72 hours from a determination that a cybersecurity event has occurred and either: requires notice to be provided to any government body, self-regulatory agency, or any other supervisory body; or, has a reasonable likelihood of materially harming any material part of the normal operation(s) of the organization.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	In the event of a breach that must be reported to affected individuals, the organization notifies affected individuals through written notification by first-class mail, electronic mail (per a previously established and valid agreement), via next of kin if the organization knows the individual(s) is/are deceased, or a substitute form of notice reasonably calculated to reach the individual(s) as required by law. In any case deemed by the organization to require urgency because of possible imminent misuse of unsecured PHI, the covered entity provides information to individuals by telephone or other means, as appropriate, in addition to the initial notice. The organization's notifications to individuals affected by security events are written in plain language.
Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation (example):	The licensee reports, at least annually, the overall status and compliance of the information security program, and any matters relevant to the program (e.g., risk assessments, events, violations, etc.). The licensee is required to notify the director no later than 72 hours after notification of a cybersecurity event if South Carolina is the licensee's state of domicile, or the licensee's home state in the case of a producer; or the Licensee has reason to believe the information involved in the event involves no less than 250 consumers residing in the State and there is reasonable likelihood of harm to consumer residing in the State.
Level CCPA Implementation Requirements	
Level CCPA Implementation (example):	Businesses notify consumers if there is unauthorized access to the consumer's non-encrypted or non-redacted personal information due to the business's lack of sufficient security controls.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization employs automated mechanisms to assist in the reporting of security incidents.

	The organization develops an incident response plan that: provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and mature an incident response capability; and is reviewed and approved by the applicable Incident Response Team Leader. The organization distributes copies of the incident response plan to CMS Chief Information Security Officer, CMS Chief Information Officer, Information System Security Officer, CMS Office of the Inspector General/Computer Crimes Unit, all personnel within the organization Incident Response Team, all personnel within the PII Breach Response Team, all personnel within the organization Operations Centers. The organization: reviews the incident response plan within every 365 days; updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; communicates incident response plan changes to the designated organizational elements; protects the incident response plan from unauthorized disclosure and modification.
Level TX-RAMP Implementation Requirements	
Level TX-RAMP Implementation (example):	The organization requires personnel to report suspected incidents to the organizational incident response capability within 48 hours of discovery, and report incident information to the Texas Department of Information Resources if the incident involves state of Texas confidential information.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization, acting as a health information custodian, provides notice to individuals of their right to make a complaint to designated government authorities, in the event PHI about an individual that is in the custody or control of the organization is stolen, lost, used, disclosed, or collected without authority. The organization provides notice to the individual and designated government authorities when personal health information about an individual that is in the organization's custody or control is stolen, lost, or if it is used or disclosed without authority.

Control Reference: 11.b Reporting Security Weaknesses

Control Specification:	All employees, contractors, and third-party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA CMS Minimum Security Requirements (High)

Level 1 Implementation (example):	The organization has an easy-to-use, available, and widely accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC2.3 AICPA Trust Services Criteria - AICPA 2017 P6.5 Banking Requirements - FFIEC IS v2016 A.8.5(g) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SI-02 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(B) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) IRS Pub 1075 - PE-17d ISO/IEC 27002:2022 - 6(8) ISO/IEC 27799:2016 16.1.3 NIST Cybersecurity Framework v1.1 - RS.CO-2 NIST Cybersecurity Framework v1.1 - RS.CO-3 NIST SP 800-53 r5 - IR-6(3)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA FTC Red Flags Rule (16 CFR 681) Banking Requirements CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	All employees, contractors, and third-party users report incident and event information, including violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism is easy to use, widely accessible, and available to all employees.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC2.3 Banking Requirements - FFIEC IS v2016 A.8.1(m) Banking Requirements - FFIEC IS v2016 A.8.5(g) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PL-04 (HIGH; MOD) FTC Red Flags Rule (16 CFR 681) - 681.A2.c2 FTC Red Flags Rule (16 CFR 681) - 681.A2.c3 FTC Red Flags Rule (16 CFR 681) - 681.A2.c4 FTC Red Flags Rule (16 CFR 681) - 681.A2.c5 IRS Pub 1075 - IR-6a ISO/IEC 27799:2016 16.1.3 NIST SP 800-53 R4 IR-6(2)[S]{0} NIST SP 800-53 r5 - IR-6(2) PCI DSS v3.2.1 12.10.4 Veterans Affairs Cybersecurity Program Directive 6500 - d(2)(c)

Objective Name: 11.02 Management of Information Security Incidents and Improvements

Control Objective:	To ensure a consistent and effective approach to the management of information security incidents.

Control Reference: 11.c Responsibilities and Procedures

Control Specification:	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	

Level 1 Regulatory Factors:	DirectTrust FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) 23 NYCRR 500 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Supplemental Requirements Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 1 Implementation (example):	The organization tests and/or exercises its incident response capability regularly. The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); procedures defining roles and responsibilities; incident handling procedures (business and technical); communication; reporting and retention; and references the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation).

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.02(b)(5) 23 NYCRR 500 - 500.03(n) 23 NYCRR 500 - 500.16(a) 23 NYCRR 500 - 500.16(b)(1) 23 NYCRR 500 - 500.16(b)(2) 23 NYCRR 500 - 500.16(b)(3) 23 NYCRR 500 - 500.16(b)(4) 23 NYCRR 500 - 500.16(b)(5) 23 NYCRR 500 - 500.16(b)(6) 23 NYCRR 500 - 500.16(b)(7) AICPA Trust Services Criteria - AICPA 2017 CC7.4 AICPA Trust Services Criteria - AICPA 2017 CC7.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-05(01) (HIGH) FedRAMP - IR-4a[H] FedRAMP - IR-4a[L] FedRAMP - IR-4a[M] Health Industry Cybersecurity Practices - 10.M.A Health Industry Cybersecurity Practices - 8.M.B Health Industry Cybersecurity Practices - 8.S.A HIPAA Security Rule - § 164.308(a)(1)(i) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) ISO/IEC 27002:2022 - 5(24) MARS-E v2.2 - IR-4a NIST Cybersecurity Framework v1.1 - PR.IP-10 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - RC.CO-1 NIST Cybersecurity Framework v1.1 - RS.AN-2 NIST Cybersecurity Framework v1.1 - RS.AN-5 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-2 NIST Cybersecurity Framework v1.1 - RS.CO-3 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST Cybersecurity Framework v1.1 - RS.MI-1 NIST SP 800-171 r2 - 3.6.1[a] NIST SP 800-171 r2 - 3.6.1[b] NIST SP 800-171 r2 - 3.6.1[c] NIST SP 800-171 r2 - 3.6.1[d] NIST SP 800-171 r2 - 3.6.1[e] NIST SP 800-171 r2 - 3.6.1[f] NIST SP 800-171 r2 - 3.6.1[g] NIST SP 800-171 r2 - 3.6.2[c] NIST SP 800-171 r2 - 3.6.2[d] NIST SP 800-171 r2 - 3.6.2[e] NIST SP 800-171 r2 - 3.6.2[f] NIST SP 800-171 r2 - 3.6.3[a] NIST SP 800-53 R4 IR-4a[HML]{1} NIST SP 800-53 R4 SA-15(7)d[S]{0} NIST SP 800-53 r5 - IR-4(15) NIST SP 800-53 r5 - IR-4a NIST SP 800-53 r5 - PE-17d NIST SP 800-53 r5 - SA-15(7)d NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4[IS.4a] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4[IS.4b] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4a

Level 1 Authoritative Source Mapping (Cont.):	NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4d PCI DSS v3.2.1 12.10.6 Supplemental Requirements - SR v6.4 34-0 Supplemental Requirements - SR v6.4 34a-0 Veterans Affairs Cybersecurity Program Directive 6500 - d(4)(a) Veterans Affairs Cybersecurity Program Directive 6500 - e(3)(c)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FTC Red Flags Rule (16 CFR 681) 23 NYCRR 500 CA Civil Code § 1798.81.5 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act State of Nevada Security and Privacy of Personal Information High Low Moderate Privacy Supplemental
Level 2 Implementation (example):	The organization implements a formal incident response program, which includes the definition of specific phases for incident response and accounts for and prepares the organization for a variety of incidents (e.g., system failure or loss of service, malicious code, denial of service, errors, unauthorized disclosures of covered and/or confidential information, system misuse, unauthorized WAPs, and identity theft). In addition to normal contingency plans, the program also covers: analysis and identification of the cause of the incident; containment; increased monitoring of system use; and planning and implementation of corrective action to prevent recurrence. The organization assigns a single point of contact for the organization responsible for sharing information and coordinating responses, and has the authority to direct actions required in all phases of the incident response process.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC3.1 AICPA Trust Services Criteria - AICPA 2017 CC7.3 AICPA Trust Services Criteria - AICPA 2017 CC7.4 AICPA Trust Services Criteria - AICPA 2017 CC7.5 AICPA Trust Services Criteria - AICPA 2017 P6.3 Banking Requirements - FFIEC IS v2016 A.6.21(c) Banking Requirements - FFIEC IS v2016 A.8.5(c) Banking Requirements - FFIEC IS v2016 A.8.5(e) Banking Requirements - FFIEC IS v2016 A.8.5(f) Banking Requirements - FFIEC IS v2016 A.8.5(h) Banking Requirements - FFIEC IS v2016 A.8.6(a) Banking Requirements - FFIEC IS v2016 A.8.6(b) Banking Requirements - FFIEC IS v2016 A.8.6(c) Banking Requirements - FFIEC IS v2016 A.8.6(d) Banking Requirements - FFIEC IS v2016 A.8.6(e) Banking Requirements - FFIEC IS v2016 A.8.6(f) Banking Requirements - FFIEC IS v2016 A.8.6(g) Banking Requirements - FFIEC IS v2016 A.8.6(h) Banking Requirements - FFIEC IS v2016 A.8.6(i) CIS Controls v7.1 - CIS CSC v7.1 19.7 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-03 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-03(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 SE-02 (HIGH; MOD) COBIT 5 DS5.6 COBIT 5 DSS02.01 COBIT 5 DSS02.04 COBIT 5 DSS02.05 FedRAMP - IR-8b[H] FedRAMP - IR-8b[L] FedRAMP - IR-8b[M] FedRAMP - IR-8c[H] FedRAMP - IR-8c[L] FedRAMP - IR-8c[M] FTC Red Flags Rule (16 CFR 681) - 681.A4.a FTC Red Flags Rule (16 CFR 681) - 681.A4.b FTC Red Flags Rule (16 CFR 681) - 681.A4.c FTC Red Flags Rule (16 CFR 681) - 681.A4.d FTC Red Flags Rule (16 CFR 681) - 681.A4.e FTC Red Flags Rule (16 CFR 681) - 681.A4.f FTC Red Flags Rule (16 CFR 681) - 681.A4.g FTC Red Flags Rule (16 CFR 681) - 681.A4.h FTC Red Flags Rule (16 CFR 681) - 681.A4.i HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(D) IRS Pub 1075 - IR-3 IRS Pub 1075 - IR-3(3)a IRS Pub 1075 - IR-3(3)b IRS Pub 1075 - IR-3(3)c IRS Pub 1075 - IR-4d IRS Pub 1075 - IR-8b IRS Pub 1075 - IR-8d ISO/IEC 27002:2022 - 5(26) ISO/IEC 27002:2022 - 5(28)

Level 2 Authoritative Source Mapping (Cont.):	ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.5 ISO/IEC 27799:2016 7.10.2.1 MARS-E v2.2 - CP-4a MARS-E v2.2 - IR-3 NIST Cybersecurity Framework v1.1 - PR.IP-10 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - RC.IM-2 NIST Cybersecurity Framework v1.1 - RS.AN-2 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-3 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST Cybersecurity Framework v1.1 - RS.MI-1 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-53 R4 IR-3(2)[HM]{0} NIST SP 800-53 R4 IR-3[HM]{0} NIST SP 800-53 R4 IR-4a[HML]{2} NIST SP 800-53 R4 IR-8a[HML]{1} NIST SP 800-53 R4 IR-8a[HML]{3} NIST SP 800-53 R4 IR-8a[HML]{7} NIST SP 800-53 R4 IR-8a[HML]{8} NIST SP 800-53 R4 IR-8b[HML]{0} NIST SP 800-53 R4 IR-8c[HML]{0} NIST SP 800-53 R4 SA-12(12)[S]{0} NIST SP 800-53 R4 SE-2[P]{1} NIST SP 800-53 R4 SI-3(10)b[S]{0} NIST SP 800-53 R4 SI-3(6)b[S]{1} NIST SP 800-53 r5 - IR-3 NIST SP 800-53 r5 - IR-3(2) NIST SP 800-53 r5 - IR-4a NIST SP 800-53 r5 - IR-8a1 NIST SP 800-53 r5 - IR-8a10 NIST SP 800-53 r5 - IR-8a3 NIST SP 800-53 r5 - IR-8a7 NIST SP 800-53 r5 - IR-8a8 NIST SP 800-53 r5 - IR-8a9 NIST SP 800-53 r5 - IR-8b NIST SP 800-53 r5 - SI-3(10)b NIST SP 800-53 r5 - SI-3(6)b NIST SP 800-53 r5 - SR-8 NY OHIP Moderate-Plus Security Baseline v5.0 - IR-3 NY OHIP Moderate-Plus Security Baseline v5.0 - IR-3[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-3[IS.3] PCI DSS v3.2.1 11.1.2 PCI DSS v3.2.1 12.10.1 PCI DSS v3.2.1 12.10.2 PCI DSS v3.2.1 12.10.4 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(j) Veterans Affairs Cybersecurity Program Directive 6500 - c(1)(g) Veterans Affairs Cybersecurity Program Directive 6500 - c(1)(h) Veterans Affairs Cybersecurity Program Directive 6500 - d(1)(b) Veterans Affairs Cybersecurity Program Directive 6500 - d(5)(b) Veterans Affairs Cybersecurity Program Directive 6500 - d(5)(c) Veterans Affairs Cybersecurity Program Directive 6500 - e(3)(a)

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA Banking Requirements CMS Minimum Security Requirements (High) High Low Moderate
Level 3 Implementation (example):	The organization provides an incident response support resource who is an integral part of the organization's incident response capability and offers advice and assistance to users of information systems for the handling and reporting of security incidents. Weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. The organization: promptly reports incident information to appropriate authorities; and communicates with outside parties regarding the incident. This includes reporting incidents to organizations such as the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT), contacting law enforcement, and fielding inquiries from the media. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.8.5(f) Banking Requirements - FFIEC IS v2016 A.8.6(f) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-07 (HIGH; MOD) FedRAMP - IR-6a[H] FedRAMP - IR-6a[L] FedRAMP - IR-6a[M] FedRAMP - IR-6b[H] FedRAMP - IR-6b[L] FedRAMP - IR-6b[M] FedRAMP - IR-7(1)[H] FedRAMP - IR-7(1)[M] FedRAMP - IR-7[H] FedRAMP - IR-7[L] FedRAMP - IR-7[M] HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.316(b)(2)(ii) IRS Pub 1075 - IR-6(2) IRS Pub 1075 - IR-7 IRS Pub 1075 - IR-7(1) ISO/IEC 27799:2016 16.1.3 ISO/IEC 27799:2016 16.1.5 MARS-E v2.2 - IR-7 MARS-E v2.2 - IR-7(1) NIST Cybersecurity Framework v1.1 - RC.CO-3 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-2 NIST Cybersecurity Framework v1.1 - RS.CO-3 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST Cybersecurity Framework v1.1 - RS.CO-5 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-53 R4 IR-7(1)[HM]{0} NIST SP 800-53 R4 IR-7[HML]{0} NIST SP 800-53 r5 - IR-7 NIST SP 800-53 r5 - IR-7(1) NIST SP 800-53 r5 - RA-3(4) NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4(1)[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4(1)[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4(1)[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4(1)[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-7 NY OHIP Moderate-Plus Security Baseline v5.0 - IR-7(1) NY OHIP Moderate-Plus Security Baseline v5.0 - RA-5(11) NY OHIP Moderate-Plus Security Baseline v5.0 - RA-5(11)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2[IS.4] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-2[PHI.4] Veterans Affairs Cybersecurity Program Directive 6500 - c(3)(c)
Level CIS Implementation Requirements	
Level CIS Implementation (example):	The organization plans and conducts routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats, and exercises test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization employs automated mechanisms to assist in the tracking of security incidents. The organization distributes copies of the incident response plan to the CMS Chief Information Security Officer, CMS Chief Information Officer, Information System Security Officer, CMS Office of the Inspector General/Computer Crimes Unit, all personnel within the organization Incident Response Team, all personnel within the PII Breach Response Team, and all personnel within the organization Operations Centers. The organization communicates incident response plan changes through the distribution of information to the organizational elements listed above.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The service provider has a list of incident response personnel identified by name and/or by role, including FedRAMP personnel, and organizational element. The organization has an information spillage response capability by: assigning organization-defined personnel or roles with responsibility for responding to information spills; providing information spillage response training at least annually; ensuring that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions; and employing security safeguards for personnel exposed to information not within assigned access authorizations.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization tracks and documents all physical security incidents, and information system security incidents potentially affecting the confidentiality of FTI. The organization must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the organization must contact TIGTA and the IRS immediately, and will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization responds to information spills by: requiring personnel to report suspected incidents to the organizational incident response capability within the time frame established in the current Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling reporting process, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/; identifying the specific information involved in the improper or potentially improper information disclosure; alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill; identifying other information systems or system components on which the information may have been subsequently improperly, or potentially improperly, shared with or disclosed to; and removing and destroying the information from the contaminated information system, component, or individual not authorized to handle such information.

Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	For the purposes of determining when external parties must be notified, the organization treats security events as discovered on the first day in which the security event is or would have been known by the organization through exercising reasonable due diligence.

Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation (example):	Upon notification of a cybersecurity event, the licensee must conduct a prompt and thorough investigation of the event.
Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization develops incident detection and response procedures that include: identifying and alerting on anomalous network traffic (from lessons learned from investigations, variances to normal traffic models, anomalous behavior and other attack patterns identified by threat-hunting/data analysis); and analyzing network packets to support investigation and forensics activities. The organization develops incident response plans that include the roles and responsibilities of both internal resources and third-party service providers, including details on when third-party service providers are required to assist in investigation and response activities.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization tracks and documents all physical incidents, information security incidents, and privacy incidents. The organization investigates suspicious activity or suspected violations on the information system, reports findings to appropriate officials, and takes appropriate action.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization establishes and maintains a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours. The organization detects and prevents counterfeit components from entering the system, and reports counterfeit system components to the source of the counterfeit component, any organization-defined external reporting organizations, or any organization-defined personnel or roles.
Level HICP Implementation Requirements	
Level HICP Implementation (example):	The organization has documented in its incident management program the steps to be followed in the event of malware downloaded on a computer and upon receipt of a phishing attack.

Control Reference: 11.d Learning from Information Security Incidents

Control Specification:	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 1 System Factors:	
Level 1 Regulatory Factors:	FedRAMP FISMA 23 NYCRR 500 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 1 Implementation (example):	The information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents, and update the incident response and recovery strategy. The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, and training and testing exercises. The organization implements the resulting changes to incident response procedures, training exercises, and testing exercises accordingly.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.14(b) 23 NYCRR 500 - 500.16(b)(5) 23 NYCRR 500 - 500.16(b)(7) AICPA Trust Services Criteria - AICPA 2017 CC7.4 AICPA Trust Services Criteria - AICPA 2017 CC7.5 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-05 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-05(01) (HIGH) FedRAMP - IR-4c[H] FedRAMP - IR-4c[L] FedRAMP - IR-4c[M] FedRAMP - IR-8d[H] FedRAMP - IR-8d[L] FedRAMP - IR-8d[M] Health Industry Cybersecurity Practices - 8.M.B HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(5)(ii)(C) HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) IRS Pub 1075 - AT-2d IRS Pub 1075 - AT-3c IRS Pub 1075 - IR-8c ISO/IEC 27002:2022 - 5(27) ISO/IEC 27002:2022 - 5(7) ISO/IEC 27799:2016 16.11.6 MARS-E v2.2 - IR-4c NIST Cybersecurity Framework v1.1 - PR.PT-2 NIST Cybersecurity Framework v1.1 - RC.IM-1 NIST Cybersecurity Framework v1.1 - RC.IM-2 NIST Cybersecurity Framework v1.1 - RS.AN-2 NIST Cybersecurity Framework v1.1 - RS.AN-4 NIST Cybersecurity Framework v1.1 - RS.CO-5 NIST Cybersecurity Framework v1.1 - RS.IM-1 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST SP 800-53 R4 IR-4c[HML]{0} NIST SP 800-53 R4 IR-8a[HML]{6} NIST SP 800-53 R4 IR-8d[HML]{0} NIST SP 800-53 R4 SI-3(6)b[S]{2} NIST SP 800-53 r5 - IR-4c NIST SP 800-53 r5 - IR-8a6 NIST SP 800-53 r5 - IR-8c NIST SP 800-53 r5 - SI-3(6)b NY OHIP Moderate-Plus Security Baseline v5.0 - AT-2d NY OHIP Moderate-Plus Security Baseline v5.0 - AT-3c NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4c PCI DSS v3.2.1 12.10.6 Veterans Affairs Cybersecurity Program Directive 6500 - d(3)(a) Veterans Affairs Cybersecurity Program Directive 6500 - d(4)(d) Veterans Affairs Cybersecurity Program Directive 6500 - d(5)(a) Veterans Affairs Cybersecurity Program Directive 6500 - d(5)(b) Veterans Affairs Cybersecurity Program Directive 6500 - e(2)(a)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA 23 NYCRR 500 PCI DSS v3.2.1 State of Massachusetts Data Protection Act (201 CMR 17.00) CMS Minimum Security Requirements (High) High Low Moderate
Level 2 Implementation (example):	The organization coordinates incident handling activities with contingency planning activities.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04 (HIGH; MOD) FedRAMP - CP-2c[H] FedRAMP - CP-2c[L] FedRAMP - CP-2c[M] FedRAMP - IR-4b[H] FedRAMP - IR-4b[L] FedRAMP - IR-4b[M] HIPAA Security Rule - § 164.308(a)(6)(i) HIPAA Security Rule - § 164.308(a)(6)(ii) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) IRS Pub 1075 - CP-2c MARS-E v2.2 - CP-2c MARS-E v2.2 - IR-4b NIST SP 800-53 R4 CP-2c[HML]{0} NIST SP 800-53 R4 IR-4b[HML]{0} NIST SP 800-53 r5 - CP-2c NIST SP 800-53 r5 - IR-4b NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2c NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4(3)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - IR-4b

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization has implemented an incident handling capability using the current CMS Incident Handling and Breach Notification Standard and Procedures. Relevant information related to a security incident is documented in accordance with the CMS publication.

	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization employs automated mechanisms to assist in the collection and analysis of incident information.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization provides specific incident response guidance relative to data incidents involving FTI. Once an incident has been addressed, the organization conducts a post-incident review to ensure the incident response policies and procedures provide adequate guidance, and completes SPR section 9.11.5.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization: implements an incident handling capability (i.e., system incident response plan) using the current RMH, Chapter 08: Incident Response; coordinates incident handling activities with contingency planning activities; and incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly.

Control Reference: 11.e Collection of Evidence

Control Specification:	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction(s).
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act
Level 1 Implementation (example):	The organization collects, retains, and presents evidence to support legal action (either civil or criminal) in accordance with the laws of the relevant jurisdiction(s).
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 23 NYCRR 500 - 500.16(b)(6) FTC Red Flags Rule (16 CFR 681) - 681.A4.d HIPAA Privacy Rule - 164.530(j)(1)(iv) HIPAA Security Rule - § 164.308(a)(1)(ii)(C) ISO/IEC 27799:2016 16.1.7 NIST Cybersecurity Framework v1.1 - ID.GV-3 NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.4] Veterans Affairs Cybersecurity Program Directive 6500 - b(5)(d)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA Banking Requirements PCI DSS v3.2.1 CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Internal procedures are developed / documented and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization. To achieve admissibility of the evidence, the organization ensures that their information systems comply with any published standard or code of practice for the production of admissible evidence.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.8.1(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IR-04 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(C) ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.7 MARS-E v2.2 - IR-4a NIST Cybersecurity Framework v1.1 - RS.AN-3 NIST SP 800-53 R4 IR-10[S]{1} NIST SP 800-53 R4 IR-10[S]{2} NY OHIP Moderate-Plus Security Baseline v5.0 - AU-2[IS.4] PCI DSS v3.2.1 A1.4 Veterans Affairs Cybersecurity Program Directive 6500 - d(3)(e) Veterans Affairs Cybersecurity Program Directive 6500 - d(3)(f)
Level Cloud Service Providers Implementation Requirements	
Level Cloud Service Providers Implementation (example):	Upon notification, customers and/or other external business partners impacted by a security breach are given the opportunity to participate, as is legally permissible, in the forensic investigation.
Level PCI Implementation Requirements	
Level PCI Implementation (example):	Service providers protect each organization’s hosted environment and data by enabling a process to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

Level Community Supplemental Requirements 002 Implementation Requirements	
Level Community Supplemental Requirements 002 Implementation (example):	The organization deploys a solution to monitor and retain detailed endpoint telemetry that: records details such as trace of process execution (e.g., file paths, libraries called, sockets opened, files opened/written), network connections, file input/output, and registry changes; can implement customized detection rules to complement endpoint preventative controls and address gaps in other solutions (e.g., banning files/hashes, network connections, processes execution); and aggregates and makes data available to others for building detection rules and investigating incidents. The organization documents details on the flow of sensitive data to the individual systems, including the details on system type (e.g., manufacturer, operating system), roles (e.g., database, file server), and network location (e.g., subnet, IP address).
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization preserves evidence related to security incidents through technical means, including secured storage of evidence media and “write” protection of evidence media, uses sound forensics processes and utilities that support legal requirements, and determines and follows a chain of custody for forensic evidence. The organization, when subject to a legal investigation (e.g., Insider Threat), maintains audit records until released by the investigating authority.

Control Category: 12.0 - Business Continuity Management

Objective Name: 12.01 Information Security Aspects of Business Continuity Management

Control Objective:	To ensure that strategies and plans are in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Control Reference: 12.a Including Information Security in the Business Continuity Management Process

Control Specification:	A managed program and process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act

Level 1 Implementation (example):	The organization: identifies all the assets involved in critical business processes; considers the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management; ensures the safety of personnel and the protection of information assets and organizational property; and formulates and documents business continuity plans addressing information security requirements in line with the agreed business continuity strategy.
Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC9.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(08) (HIGH; MOD) FedRAMP - CP-2(8)[H] HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) HIPAA Security Rule - § 164.308(a)(7)(ii)(E) IRS Pub 1075 - CP-2(8) ISO/IEC 27799:2016 17.1.2 MARS-E v2.2 - CP-2(8) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(8)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(8)[IS.2]
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA 23 NYCRR 500 Banking Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental

Level 2 Implementation (example):	The organization brings together the following key information security elements of business continuity management: identifying critical information system assets supporting organizational missions and functions; understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes; understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information assets; implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible; identifying financial, organizational, technical, and environmental resources to address the identified information security requirements; testing and updating, at a minimum, a section of the plans and processes put in place at least annually; ensuring that the management of business continuity is incorporated in the organization's processes and structure; and assigning responsibility for the business continuity management process at an appropriate level within the organization.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 CC7.3 AICPA Trust Services Criteria - AICPA 2017 CC7.4 AICPA Trust Services Criteria - AICPA 2017 CC7.5 AICPA Trust Services Criteria - AICPA 2017 CC9.1 Banking Requirements - FFIEC IS v2016 A.6.35(a) Banking Requirements - FFIEC IS v2016 A.6.35(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(08) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-09 (HIGH; MOD) FedRAMP - CP-2(8)[M] HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(D) HIPAA Security Rule - § 164.308(a)(7)(ii)(E) ISO/IEC 27799:2016 17.1.2 NIST Cybersecurity Framework v1.1 - DE.AE-2 NIST Cybersecurity Framework v1.1 - DE.AE-3 NIST Cybersecurity Framework v1.1 - ID.BE-5 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - RS.AN-2 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-53 R4 CP-2(8)[HM]{0} NIST SP 800-53 R4 CP-4[HML]{0} NIST SP 800-53 R4 SA-13a[S]{2} NIST SP 800-53 R4 SA-14[S]{2} NIST SP 800-53 r5 - CP-2(8) NIST SP 800-53 r5 - CP-4 NIST SP 800-53 r5 - RA-2(1)
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	The organization implements procedures to allow facility access in support of restoration activities in emergency-related events.

Control Reference: 12.b Business Continuity and Risk Assessment

Control Specification:	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The organization identifies the critical business processes requiring business continuity.
Level 1 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(08) (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) HIPAA Security Rule - § 164.308(a)(7)(ii)(E) ISO/IEC 27799:2016 17.1.1 NIST Cybersecurity Framework v1.1 - ID.BE-5 NIST SP 800-53 r5 - PM-30(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(8) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(8)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(8)[IS.2] Veterans Affairs Cybersecurity Program Directive 6500 - a(2)(e) Veterans Affairs Cybersecurity Program Directive 6500 - a(2)(j)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust FISMA HITRUST De-ID Framework The Joint Commission v2016 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Supplemental

Level 2 Implementation (example):	Information security aspects of business continuity are: based on identifying events (or sequence of events) that can cause interruptions to the organizations critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters, and acts of terrorism); followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period; based on the results of the risk assessment, a business continuity strategy is developed to identify the overall approach to business continuity; and once this strategy has been created, endorsement is provided by management, and a plan created and endorsed to implement this strategy. The organization identifies its critical business processes and integrates the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport, and facilities.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.3 AICPA Trust Services Criteria - AICPA 2017 CC3.3 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PM-08 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(E) HITRUST De-ID Framework - De-ID Framework v1 Physical and Environmental Security: General ISO/IEC 27001:2022 - 6.1.2c2 ISO/IEC 27002:2022 - 5(29) ISO/IEC 27799:2016 17.1.1 ISO/IEC 27799:2016 17.1.2 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - DE.AE-4 NIST Cybersecurity Framework v1.1 - ID.AM-5 NIST Cybersecurity Framework v1.1 - ID.BE-2 NIST Cybersecurity Framework v1.1 - ID.BE-4 NIST Cybersecurity Framework v1.1 - ID.BE-5 NIST Cybersecurity Framework v1.1 - ID.RA-3 NIST Cybersecurity Framework v1.1 - ID.RA-4 NIST Cybersecurity Framework v1.1 - ID.RA-5 NIST SP 800-53 R4 SI-13a[S]{2} NIST SP 800-53 r5 - SI-13a Veterans Affairs Cybersecurity Program Directive 6500 - d(3)(d)

Level ISO/IEC 23894 Implementation Requirements

Level ISO/IEC 23894 Implementation (example):	The organization conducts business impact analyses on AI systems at a minimum annually, considering the criticality of the impact, tangible and intangible impacts, and criteria used to establish the overall impact.

Control Reference: 12.c Developing and Implementing Continuity Plans Including Information Security

Control Specification:	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information, at the required level and in the required time scales, following interruption to, or failure of, critical business processes.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust PCI DSS v3.2.1 Texas Medical Records Privacy Act High Low Moderate
Level 1 Implementation (example):	Business continuity plans: identify the necessary capacity for information processing during contingency operations, e.g., during an information system disruption, compromise or failure; identify the necessary capacity for telecommunications during contingency operations; identify the necessary capacity for environmental support during contingency operations; identify the essential missions and business functions; identify the contingency requirements associated with essential missions and business functions; provide recovery objectives; provide restoration priorities; provide recovery and restoration metrics; address contingency roles; assign individuals to contingency responsibilities; and contain the contact information of individuals assigned to contingency responsibilities.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.03(e) 23 NYCRR 500 - 500.06(a)(1) 23 NYCRR 500 - 500.16(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(05) (HIGH) FedRAMP - CP-2a1[H] FedRAMP - CP-2a1[L] FedRAMP - CP-2a1[M] FedRAMP - CP-2a2[H] FedRAMP - CP-2a2[L] FedRAMP - CP-2a2[M] FedRAMP - CP-2a3[H] FedRAMP - CP-2a3[L] FedRAMP - CP-2a3[M] FedRAMP - CP-2a4[H] FedRAMP - CP-2a4[L] FedRAMP - CP-2a4[M] HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) HIPAA Security Rule - § 164.308(a)(7)(ii)(E) HIPAA Security Rule - § 164.312(a)(2)(ii) IRS Pub 1075 - CP-2a1 IRS Pub 1075 - CP-2a2 IRS Pub 1075 - CP-2a3 IRS Pub 1075 - CP-2a4 ISO/IEC 27002:2022 - 5(30) NIST Cybersecurity Framework v1.1 - ID.BE-4 NIST Cybersecurity Framework v1.1 - ID.BE-5 NIST Cybersecurity Framework v1.1 - RC.RP-1 NIST SP 800-53 R4 CP-2a[HML]{2} NIST SP 800-53 R4 CP-2a[HML]{3} NIST SP 800-53 R4 CP-2a[HML]{4} NIST SP 800-53 r5 - CP-2a2 NIST SP 800-53 r5 - CP-2a3 NIST SP 800-53 r5 - CP-2a4 The Joint Commission (v2016) - TJC IM.01.01.03, EP 2 The Joint Commission (v2016) - TJC IM.01.01.03, EP 4 Veterans Affairs Cybersecurity Program Directive 6500 - e(1)(c)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	DirectTrust HITRUST De-ID Framework The Joint Commission v2016 Banking Requirements PCI DSS v3.2.1 Texas Medical Records Privacy Act High Low Moderate
Level 2 Implementation (example):	The business continuity planning process includes the following: recovery and restoration of business operations and establishing an availability of information in a time frame specified by the organization; particular attention is given to the assessment of internal and external business dependencies and the contracts in place; documentation of agreed procedures and processes; and testing and updating of at least a section of the plans. The planning process focuses on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable amount of time). The procedures for obtaining necessary electronic covered and/or confidential information during an emergency are defined. The services and resources facilitating this are identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. Following an interruption to business operations, full information system restoration without deterioration of the security measures originally planned and implemented can be achieved. Copies of the business continuity plans are distributed to the Information System Security Officer (or the organization's functional equivalent), System Owner (or the organization's functional equivalent), Contingency Plan Coordinator (or the organization's functional equivalent), System Administrator (or the organization's functional equivalent), and Database Administrator (or the organization's functional equivalent).

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.35(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02(05) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-10(04) (HIGH) FedRAMP - CP-2b[H] FedRAMP - CP-2b[L] FedRAMP - CP-2b[M] HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.308(a)(7)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) HITRUST De-ID Framework - De-ID Framework v1 Physical and Environmental Security: General IRS Pub 1075 - CP-2b ISO/IEC 27002:2022 - 7(11) ISO/IEC 27799:2016 11.2.2 ISO/IEC 27799:2016 17.1.2 Legacy Inheritance Support - L.I.S. MARS-E v2.2 - CP-2b MARS-E v2.2 - CP-6(3) NIST Cybersecurity Framework v1.1 - ID.BE-4 NIST Cybersecurity Framework v1.1 - ID.BE-5 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - RC.RP-1 NIST Cybersecurity Framework v1.1 - RS.MI-2 NIST SP 800-53 R4 CP-2b[HML]{0} NIST SP 800-53 r5 - CP-2a6 NIST SP 800-53 r5 - CP-2b NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(3) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(3)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(3)[IS.2] The Joint Commission (v2016) - TJC IM.01.01.03, EP 1 The Joint Commission (v2016) - TJC IM.01.01.03, EP 2 The Joint Commission (v2016) - TJC IM.01.01.03, EP 3 The Joint Commission (v2016) - TJC IM.01.01.03, EP 4

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Licensed Beds: Greater than 750 Beds Number of Covered Lives: Greater than 7.5 Million Lives Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of transactions received and sent annually: More than 6 Million Transactions Number of Admitted Patients annually: More than 20k Patients Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Total Terabytes of Data Held: More than 60 Terabytes(TB) Volume of Data Exchanged Annually: More than 100 Megabytes(MB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of prescriptions filled annually: Greater than 60 million Prescriptions Number of Physicians on staff: Greater than 25 Physicians Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Patient Encounters Annually: Greater than 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Individual Records that are processed annually: More than 725k Records Number of Records that are currently held: More than 60 Million Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	FedRAMP FISMA HITRUST De-ID Framework The Joint Commission v2016 Banking Requirements CMS Minimum Security Requirements (High) High Low Moderate Supplemental
Level 3 Implementation (example):	The organization identifies alternative temporary locations for processing. The necessary third-party service agreements are established to allow for the transfer and resumption of information systems operations of critical business functions within a time period (e.g., priority of service provisions) as defined by a risk assessment. The alternate location is at a sufficient distance to escape any damage from a disaster at the main site. The organizations alternate processing site agreements contain priority-of-service provisions in accordance with the organizations availability requirements, including Recovery Time Objectives (RTOs). The alternate processing site is configured with security measures equivalent to the primary site. The organization establishes alternate telecommunications services, including necessary agreements to permit the resumption of information system operations for essential missions and business functions within a business-defined time period, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. The organization: develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and requests telecommunications service priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.2 Banking Requirements - FFIEC IS v2016 A.6.35(b) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-06 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-06(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-06(02) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-07 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-07(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-07(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-08 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-08(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-08(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-08(03) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-08(04) (HIGH) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-09(02) (HIGH) FedRAMP - CP-2(1)[H] FedRAMP - CP-2(1)[M] FedRAMP - CP-6(1)[H] FedRAMP - CP-6(1)[M] FedRAMP - CP-7(1)[H] FedRAMP - CP-7(1)[M] FedRAMP - CP-7(3)[H] FedRAMP - CP-7(3)[M] FedRAMP - CP-7(4)[H] FedRAMP - CP-7a[H] FedRAMP - CP-7a[M] FedRAMP - CP-7c[H] FedRAMP - CP-7c[M] FedRAMP - CP-8(1)a[H] FedRAMP - CP-8(1)a[M] FedRAMP - CP-8(1)b[H] FedRAMP - CP-8(1)b[M] FedRAMP - CP-8[H] FedRAMP - CP-8[M] HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(A) HIPAA Security Rule - § 164.308(a)(7)(ii)(B) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) HIPAA Security Rule - § 164.308(a)(7)(ii)(D) HIPAA Security Rule - § 164.310(a)(2)(i) HITRUST De-ID Framework - De-ID Framework v1 Physical and Environmental Security: General IRS Pub 1075 - CP-2(1) ISO/IEC 27002:2022 - 8(14) ISO/IEC 27799:2016 11.2.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2.2 - CP-10 MARS-E v2.2 - CP-6(1) MARS-E v2.2 - CP-7(1) MARS-E v2.2 - CP-7(3) MARS-E v2.2 - CP-7a MARS-E v2.2 - CP-7b MARS-E v2.2 - CP-7c MARS-E v2.2 - CP-8(1)a MARS-E v2.2 - CP-8(1)b NIST Cybersecurity Framework v1.1 - ID.BE-4 NIST Cybersecurity Framework v1.1 - ID.BE-5 NIST Cybersecurity Framework v1.1 - PR.PT-4 NIST Cybersecurity Framework v1.1 - RC.RP-1 NIST SP 800-53 R4 CP-11[S]{0}

Level 3 Authoritative Source Mapping (Cont.):	NIST SP 800-53 R4 CP-2(1)[HM]{0} NIST SP 800-53 R4 CP-2a[HML]{1} NIST SP 800-53 R4 CP-6(1)[HM]{0} NIST SP 800-53 R4 CP-6[HM]{0} NIST SP 800-53 R4 CP-7(1)[HM]{0} NIST SP 800-53 R4 CP-7(3)[HM]{0} NIST SP 800-53 R4 CP-7(4)[H]{0} NIST SP 800-53 R4 CP-7[HM]{0} NIST SP 800-53 R4 CP-8(1)[HM]{0} NIST SP 800-53 R4 CP-9(6)[S]{0} NIST SP 800-53 R4 PE-17c[HM]{1} NIST SP 800-53 R4 SC-24[H]{0} NIST SP 800-53 R4 SC-36[S]{0} NIST SP 800-53 r5 - CP-11 NIST SP 800-53 r5 - CP-2(1) NIST SP 800-53 r5 - CP-2a1 NIST SP 800-53 r5 - CP-6 NIST SP 800-53 r5 - CP-6(1) NIST SP 800-53 r5 - CP-7 NIST SP 800-53 r5 - CP-7(1) NIST SP 800-53 r5 - CP-7(3) NIST SP 800-53 r5 - CP-7(4) NIST SP 800-53 r5 - CP-8(1) NIST SP 800-53 r5 - CP-9(6) NIST SP 800-53 r5 - SA-8(24) NIST SP 800-53 r5 - SC-24 NIST SP 800-53 r5 - SC-36 NIST SP 800-53 r5 - SC-36(2) NIST SP 800-53 r5 - SC-47 NY OHIP Moderate-Plus Security Baseline v5.0 - CP-10 NY OHIP Moderate-Plus Security Baseline v5.0 - CP-10[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-10[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-10[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-10[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-10[IS.1e] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6a NY OHIP Moderate-Plus Security Baseline v5.0 - CP-6b NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7(1) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7(1)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7(1)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7(3) NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7(3)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7[IS.4] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-7c NY OHIP Moderate-Plus Security Baseline v5.0 - CP-8 NY OHIP Moderate-Plus Security Baseline v5.0 - CP-8(1)[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-8(1)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-8(1)a NY OHIP Moderate-Plus Security Baseline v5.0 - CP-8(1)b The Joint Commission (v2016) - TJC IM.01.01.03, EP 1 The Joint Commission (v2016) - TJC IM.01.01.03, EP 2 The Joint Commission (v2016) - TJC IM.01.01.03, EP 3 Veterans Affairs Cybersecurity Program Directive 6500 - e(1)(b)

Level 3 Authoritative Source Mapping (Cont.):	
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions. The organization ensures all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs). The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential CMS missions and business functions.
Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	The organization requires all critical services to be operational with a defined RPO (recovery point objective) and RTO (recovery time objective) that does not exceed 48 hours.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization requires service providers to define a time period consistent with the Recovery Time Objectives (RTOs) and Business Impact Analysis (BIA) for alternative processing sites. The organization's Service Level Agreements (SLAs) permit telecommunications service providers to resume information system operations for essential missions and business functions with the Recovery Time Objectives (RTOs) documented in a Business Impact Analysis (BIA) when primary telecommunications capabilities are unavailable.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization identifies alternative storage sites and initiates necessary agreements to permit the secure storage of information system and FTI backups and ensures the alternative storage sites provide information security safeguards that meet the minimum FTI protection and disclosure provisions of IRS 6103.
Level HIX Implementation Requirements	
Level HIX Implementation (example):	The organization ensures all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one week of contingency plan activation. The organization ensures alternate telecommunications Service Level Agreements (SLAs) are in place to permit resumption of information system operations for essential missions and business functions within a system owner-defined, business owner-approved time period consistent with the Recovery Time Objectives, Maximum Tolerable Downtimes (MTDs) and business impact analysis for the system when primary telecommunications capabilities are unavailable.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization develops a contingency plan for the information system in accordance with NIST SP 800-34 that: identifies essential CMS missions and business functions and associated contingency requirements; provides recovery objectives, restoration priorities, and metrics; addresses contingency roles and responsibilities, and assigns these to specific individuals with contact information; addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and is reviewed and approved by designated officials within the organization. The organization communicates contingency plan changes to key contingency personnel, system administrator, database administrator, and other personnel/roles as appropriate and defined organizational elements.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The information system implements transaction recovery for systems that are transaction-based. The organization identifies alternative sources of information for organization-defined essential functions and services.

Control Reference: 12.d Business Continuity Planning Framework

Control Specification:	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA The Joint Commission v2016 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 1 Implementation (example):	The organization creates, at a minimum, one business continuity plan. The organization ensures each plan: has an owner; describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security; specifies the escalation plan; specifies the conditions for the escalation plan's activation; and specifies the individuals responsible for executing each component of the plan.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) 23 NYCRR 500 - 500.02(a) 23 NYCRR 500 - 500.03(f) Banking Requirements - FFIEC IS v2016 A.6.35(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.312(a)(2)(ii) ISO/IEC 27799:2016 17.1.2 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - PR.PT-5 The Joint Commission (v2016) - TJC IM.01.01.03, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FISMA The Joint Commission v2016 Texas Medical Records Privacy Act CMS Minimum Security Requirements (High)
Level 2 Implementation (example):	When new requirements are identified, any existing emergency procedures (e.g., evacuation plans or fallback arrangements) are amended as appropriate. The organization ensures emergency procedures, manual “fallback” procedures, and resumption plans are within the responsibility of the owner of the business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, are usually the responsibility of the service providers.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) 1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) Banking Requirements - FFIEC IS v2016 A.6.35(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(C) ISO/IEC 27799:2016 17.1.2 Legacy Inheritance Support - L.I.S. NIST Cybersecurity Framework v1.1 - PR.IP-7 NIST Cybersecurity Framework v1.1 - PR.IP-9 NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(3)[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(3)[IS.3] NY OHIP Moderate-Plus Security Baseline v5.0 - CP-2(3)[IS.4] The Joint Commission (v2016) - TJC IM.01.01.03, EP 1

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Supplemental Requirements
Level 3 Implementation (example):	The business continuity planning framework addresses the identified information security requirements, temporary operational procedures to follow pending completion of recovery and restoration, and the responsibilities of the individuals, describing who is responsible for executing which component of the plan (alternatives are nominated as required).
Level 3 Authoritative Source Mapping:	HIPAA Security Rule - § 164.308(a)(7)(ii)(C) HIPAA Security Rule - § 164.310(a)(2)(i) ISO/IEC 27799:2016 17.1.2 NIST Cybersecurity Framework v1.1 - PR.IP-9 Supplemental Requirements - SR v6.4 15a-1
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization develops a contingency plan for the information system that addresses the sharing of contingency information.

Control Reference: 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans

Control Specification:	Business continuity plans shall be tested and updated regularly, at a minimum annually, to ensure that they are up to date and effective.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	The Joint Commission v2016 Texas Medical Records Privacy Act
Level 1 Implementation (example):	Responsibility is assigned for regular reviews of at least a part of the business continuity plan at a minimum, annually.
Level 1 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) ISO/IEC 27799:2016 17.1.3

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	DirectTrust EHNAC FedRAMP FISMA The Joint Commission v2016 Banking Requirements Texas Medical Records Privacy Act High Low Moderate
Level 2 Implementation (example):	Business continuity plan testing ensures that all members of the recovery team and other relevant staff are aware of the plans and their responsibilities for business continuity and information security and know their roles when a plan is invoked. The test schedule for business continuity plan(s) indicate how each element of the plan is tested, and when each element of the plan is tested.

Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) AICPA Trust Services Criteria - AICPA 2017 A1.3 Banking Requirements - FFIEC IS v2016 A.6.35(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-04(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-04(02) (HIGH) FedRAMP - CP-2e[H] FedRAMP - CP-2e[L] FedRAMP - CP-2e[M] FedRAMP - CP-4(1)[H] FedRAMP - CP-4(1)[M] HIPAA Security Rule - § 164.308(a)(7)(i) HIPAA Security Rule - § 164.308(a)(7)(ii)(D) IRS Pub 1075 - CP-2e IRS Pub 1075 - CP-4(1) ISO/IEC 27799:2016 17.1.3 MARS-E v2.2 - CP-2(1) MARS-E v2.2 - CP-2e MARS-E v2.2 - CP-4(1) NIST Cybersecurity Framework v1.1 - PR.IP-10 NIST Cybersecurity Framework v1.1 - PR.IP-7 NIST Cybersecurity Framework v1.1 - PR.IP-9 NIST Cybersecurity Framework v1.1 - RC.IM-1 NIST Cybersecurity Framework v1.1 - RC.IM-2 NIST Cybersecurity Framework v1.1 - RS.CO-1 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST Cybersecurity Framework v1.1 - RS.IM-1 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST SP 800-53 R4 CP-2e[HML]{0} NIST SP 800-53 R4 CP-4(1)[HML]{0} NIST SP 800-53 r5 - CP-2e NIST SP 800-53 r5 - CP-2g NIST SP 800-53 r5 - CP-4(1) NIST SP 800-53 r5 - CP-4(5) NY OHIP Moderate-Plus Security Baseline v5.0 - PE-12[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-13[IS.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PE-15[IS.1] The Joint Commission (v2016) - TJC IM.01.01.03, EP 5 Veterans Affairs Cybersecurity Program Directive 6500 - b(7)(a)
Level 3 Implementation Requirements	
Level 3 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 3 System Factors:	

Level 3 Regulatory Factors:	DirectTrust EHNAC FedRAMP FISMA Banking Requirements High Low Moderate
Level 3 Implementation (example):	The organization ensures the complete continuity plan is reviewed annually. The updated continuity plans are distributed to the appropriate stakeholders.
Level 3 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(4)(A)(xi) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 CP-02 (HIGH; MOD) FedRAMP - CP-2a6[H] FedRAMP - CP-2a6[L] FedRAMP - CP-2a6[M] FedRAMP - CP-2d[H] FedRAMP - CP-2d[L] FedRAMP - CP-2d[M] FedRAMP - CP-2f[H] FedRAMP - CP-2f[L] FedRAMP - CP-2f[M] HIPAA Security Rule - § 164.308(a)(7)(ii)(D) IRS Pub 1075 - CP-2a7 IRS Pub 1075 - CP-2d IRS Pub 1075 - CP-2f ISO/IEC 27799:2016 17.1.3 MARS-E v2.2 - CP-2d MARS-E v2.2 - CP-2f NIST Cybersecurity Framework v1.1 - RC.CO-3 NIST Cybersecurity Framework v1.1 - RC.IM-2 NIST Cybersecurity Framework v1.1 - RS.CO-4 NIST Cybersecurity Framework v1.1 - RS.CO-5 NIST Cybersecurity Framework v1.1 - RS.IM-2 NIST SP 800-53 R4 CP-2a[HML]{6} NIST SP 800-53 R4 CP-2d[HML]{0} NIST SP 800-53 r5 - CP-2a7 NIST SP 800-53 r5 - CP-2d
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources, and to evaluate the site’s capabilities to support contingency operations.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation (example):	The organization tests backup information at least monthly to verify media reliability and information integrity. The organization provides the capability to restore information system components within time-period consistent with the restoration time-periods defined in the service provider and organization SLA from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization has: incremental data backup procedures to validate disaster recovery and business process continuity; special purpose data backup procedures to validate disaster recovery and business process continuity; off-site storage protections to validate disaster recovery and business process continuity; and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are: bound by organization policy, and tested and verified.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization: tests the contingency plan for the information system within every 365 days using NIST (NIST SP 800-34, NIST SP 800-84) and CMS-defined tests and exercises, such as tabletop tests, in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan; reviews the contingency plan test results; and initiates corrective actions, if needed. The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Control Category: 13.0 - Privacy Practices

Objective Name: 13.01 Transparency

Control Objective:	Policies, procedures, and technologies that directly affect data subjects and/or their PII are open and transparent.

Control Reference: 13.a Privacy Notice

Control Specification:	Data Subjects have a right to adequate and easily accessible notice of the use and disclosures of their PII that may be made by the PII controller, and of the data subject's rights and the controller's legal duties with respect to PII.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust
Level 1 Implementation (example):	PII controllers provide a plain-language notice to data subjects: which outline the controller's practices and policies regarding PII; in a manner and time frame required by applicable law and/or regulation; and in a manner that can be understood by individuals not familiar with information technologies, legal jargon and the Internet. PII controllers revise their notices to reflect any changes in their practices, policies or activities that affect PII, before or as soon as practicable after the change.

Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 CC2.2 AICPA Trust Services Criteria - AICPA 2017 P1.1 APEC Cross-Border Privacy Rules (CBPR) - APEC II 15 APEC Cross-Border Privacy Rules (CBPR) - APEC II 16 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 TR-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 TR-03 (HIGH; MOD) EU GDPR Article 13(1) EU GDPR Article 14(1) HIPAA Privacy Rule - 164.520(a)(1) HIPAA Privacy Rule - 164.520(b)(1) HIPAA Privacy Rule - 164.520(b)(1)(i) HIPAA Privacy Rule - 164.520(b)(1)(ii)(A) HIPAA Privacy Rule - 164.520(b)(1)(ii)(B) HIPAA Privacy Rule - 164.520(b)(1)(ii)(C) HIPAA Privacy Rule - 164.520(b)(1)(ii)(D) HIPAA Privacy Rule - 164.520(b)(1)(ii)(E) HIPAA Privacy Rule - 164.520(b)(1)(iii)(A) HIPAA Privacy Rule - 164.520(b)(1)(iii)(B) HIPAA Privacy Rule - 164.520(b)(1)(iii)(C) HIPAA Privacy Rule - 164.520(b)(1)(iv)(A) HIPAA Privacy Rule - 164.520(b)(1)(iv)(B) HIPAA Privacy Rule - 164.520(b)(1)(iv)(C) HIPAA Privacy Rule - 164.520(b)(1)(iv)(D) HIPAA Privacy Rule - 164.520(b)(1)(iv)(E) HIPAA Privacy Rule - 164.520(b)(1)(iv)(F) HIPAA Privacy Rule - 164.520(b)(1)(v)(A) HIPAA Privacy Rule - 164.520(b)(1)(v)(B) HIPAA Privacy Rule - 164.520(b)(1)(v)(C) HIPAA Privacy Rule - 164.520(b)(1)(vi) HIPAA Privacy Rule - 164.520(b)(1)(vii) HIPAA Privacy Rule - 164.520(b)(1)(viii) HIPAA Privacy Rule - 164.520(b)(2)(i) HIPAA Privacy Rule - 164.520(b)(2)(ii) HIPAA Privacy Rule - 164.520(b)(3) HIPAA Privacy Rule - 164.520(c) HIPAA Privacy Rule - 164.520(c)(2)(iii)(A) HIPAA Privacy Rule - 164.520(c)(2)(iii)(B) HIPAA Privacy Rule - 164.520(c)(3)(i) HIPAA Privacy Rule - 164.520(c)(3)(ii) HIPAA Privacy Rule - 164.520(c)(3)(iii) HIPAA Privacy Rule - 164.530(i)(2)(i) HIPAA Privacy Rule - 164.530(i)(2)(iii) HIPAA Privacy Rule - 164.530(i)(4)(i)(A) HIPAA Privacy Rule - 164.530(i)(4)(i)(C) ISO/IEC 29100:2011 5.8 NIST SP 800-53 r5 - PT-5(1) Ontario Personal Health Information Protection Act - 18(6)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Privacy
Level 2 Implementation (example):	Requirements have been defined for ensuring, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, a close alignment between the general authorization and any specific collection of PII when statutory language is written broadly and subsequently subject to interpretation. Once the specific purposes have been identified, the organization clearly describes the purposes of collection in: related privacy compliance documentation; privacy impact assessments (PIAs) as applicable to the organization, provided at the time of collection (e.g., on forms organizations use to collect PII); System of Records Notices (SORNs) as applicable to the organization, provided at the time of collection (e.g., on forms organizations use to collect PII); and Privacy Act Statements as applicable to the organization, provided at the time of collection (e.g., on forms organizations use to collect PII). Requirements have been defined for providing real-time and/or layered notice when the organization collects PII.
Level 2 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AP-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 TR-01(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 TR-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 TR-02(01) (HIGH; MOD) MARS-E v2.2 - TR-1(1) MARS-E v2.2 - TR-2a MARS-E v2.2 - TR-2b MARS-E v2.2 - TR-2c NIST SP 800-53 R4 TR-1(1)[P]{0} NIST SP 800-53 R4 TR-2(1)[P]{0} NIST SP 800-53 R4 TR-2[P]{0} NIST SP 800-53 r5 - PT-5(2) NIST SP 800-53 r5 - PT-6 NIST SP 800-53 r5 - PT-6(1) NIST SP 800-53 r5 - PT-6(2) NIST SP 800-53 r5 - PT-8

Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	HIPAA Covered Entities must document having addressed each of the following: Notice of Privacy Practices; Right of Access to PHI; Request to Amend PHI; Request for Alternative Communication of PHI; Accounting for Disclosures of PHI; Requests for Restriction of PHI; Complaints About Privacy Practices; and Free Exercise of Privacy Rights. Business Associates handling PHI on behalf of one or more Covered Entities must address each of the foregoing elements, as required.

Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The PII controller provides data subjects with notice that is easily accessible, easily understood, and available in writing, electronically, or orally if requested. Particular care is taken to ensure the language is clear and plain if the notice is used for children. The PII controller provides data subjects with notice in a reasonable time given the type of data and use thereof (this must be within a month of the data collection). If the data is used to contact the data subject, the notice will be given when the data subject is contacted. If the data is being shared, the notice will be provided before the sharing occurs. An additional or new notice must be provided to the data subject before using the data for a different purpose than that of the original collection.
Level Group Health Plans Implementation Requirements	
Level Group Health Plans Implementation (example):	The health insurance issuer, or HMO, provides an individual (other than an inmate enrolled in a group health plan), a notice of privacy practices for the portion of the group health plan the individual receives benefits. The health notice is: provided to the named insured and one or more dependents; provided to new enrollees at the time of enrollment; and provided again within 60 days of any material revision to the notice. At a minimum of once every three years, the health plan notifies individuals, covered by the plan, of the availability of the notice and how to obtain the notice.
Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation (example):	The organization ensures that a parent of a minor child retains the rights and duties specified in Texas Family Code §§ 151.001, 153.073, 153.074 and 153.132 pursuant to the exceptions provided by Texas Family Code §§ 32.003 through 32.005. A parent, foster parent, guardian, or managing conservator of a minor child with special healthcare needs or an adult client with special needs retains the rights and duties specified in 25 Texas Admin. Code § 38.5.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	If the organization, acting as a covered entity, provides a health plan, the organization provides notice(s) relevant to the individual (other than an inmate) no later than the compliance date or upon enrollment thereafter, within 60 days of a material revision, and no less than every three years. An organization, acting as a covered entity, may provide individuals the privacy notice by email, if the individual agrees to electronic notice and the agreement has not been withdrawn.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization: provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

	The organization provides effective notice to the public and to individuals regarding: its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); authority for collecting PII; the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and the ability to access and have PII amended or corrected if necessary. The organization describes: the PII the organization collects and the purpose(s) for which it collects that information; how the organization uses PII internally; whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to PII; and how the PII will be protected. The organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization does not charge an individual a fee for collecting or using personal health information except as authorized by law.
Control Reference: 13.b Openness and Transparency	
Control Specification:	To provide data subjects with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the handling of PII.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	CCPA GDPR Privacy
Level 1 Implementation (example):	PII controllers provide data subjects with clear and easily accessible information about the policies, procedures, and practices with respect to the processing of PII. PII controllers disclose the choices and means available to the data subject for the purpose of limiting the processing of their PII, accessing their PII, correcting their PII, and removing their PII. Organizations provide effective notice to data subjects regarding: its activities that impact privacy including, but not limited to, the collection, use, sharing, safeguarding, maintenance, and disposal of PII; authority for collecting PII; the PII collected, the purpose(s) for which it is collected and how it will be protected; the choice, if any, data subject may have regarding how the PII controller uses PII and the consequence of exercising or not exercising those choices; the ability to object to the processing; if the PII controller intends to levy any fees for access, as may be permitted by law in some jurisdictions; how long the PII will be retained; how data subjects may obtain access to their PII for the purpose of amendment or correction, where appropriate; whether the PII controller shares PII with external entities and the purposes for such sharing; whether the organization on-sells or forwards the data for processing by data analytics organizations and the details applicable to PII risks; and how data subjects are able to communicate with the organization's privacy officials to provide feedback, including but not limited to complaints and/or direct questions regarding privacy practices.

Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P1.1 AICPA Trust Services Criteria - AICPA 2017 P2.1 AICPA Trust Services Criteria - AICPA 2017 P6.7 AICPA Trust Services Criteria - AICPA 2017 P8.1 APEC Cross-Border Privacy Rules (CBPR) - APEC II 15 APEC Cross-Border Privacy Rules (CBPR) - APEC II 15(a) APEC Cross-Border Privacy Rules (CBPR) - APEC II 15(b) APEC Cross-Border Privacy Rules (CBPR) - APEC II 15(c) APEC Cross-Border Privacy Rules (CBPR) - APEC II 15(d) APEC Cross-Border Privacy Rules (CBPR) - APEC II 15(e) APEC Cross-Border Privacy Rules (CBPR) - APEC II 16 CCPA 1798.100(b) CCPA 1798.110(a) EU GDPR Article 13(1) EU GDPR Article 13(1)(a) EU GDPR Article 13(1)(c) EU GDPR Article 14(1) ISO/IEC 29100:2011 5.8 NIST SP 800-53 R4 TR-3b[P]{0} NIST SP 800-53 R4 UL-2a[P]{0} NIST SP 800-53 r5 - PM-20 NIST SP 800-53 r5 - PT-5 Ontario Personal Health Information Protection Act - 18(6) Singapore Personal Data Protection Act - PDPA 11(5) Singapore Personal Data Protection Act - PDPA 20(1)(e)
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	An adequate privacy notice includes information on data retention, includes information on data subject rights, information on available remedies, contact information for the controller, contact information on, if applicable, the data protection officer, information on the purposes of the processing, information on the legal basis for processing, information on the categories of data concerned, information on the recipients or types of recipients of the data, and information on, if applicable, information about transfers outside the EEA. If automated decision-making including profiling will be done, the data subject must be informed of this. If automated decision-making including profiling will be done, the data subject must be informed of the potential consequences of the profiling or of not providing the necessary information.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	The organization, acting as a covered entity, provides individuals with an appropriate notice of the potential uses and disclosures of their PHI that contains the required elements.
Level Personal Data Protection Act Implementation Requirements	
Level Personal Data Protection Act Implementation (example):	If a controller receives data from another controller, the receiving controller informs the original controller of the purposes for which the data is to be used, to ensure proper consent has been obtained. The controller notifies the data subject if information is to be used in regard to an employment relationship. If requested, the controller provides the data subject with the contact information of someone able to answer any additional questions from the data subject. Telecommunications providers notify the PDPC of terminated numbers. Telecommunications providers must register with the PDPC before submitting its first information on discontinued numbers.

Level CCPA Implementation Requirements	
Level CCPA Implementation (example):	Consumers are notified of their right to request deletion. Businesses disclose in their notice to consumers their practices relating to the selling or disclosing of information.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization, acting as a health information custodian, makes available to the public a written statement that describes how an individual may obtain access to or request correction of a record of PHI about the individual that is in the custody or control of the organization and describes how to make a complaint to the custodian and to the Commissioner. The organization, acting as a health information custodian, makes available to the public a written statement that describes how to contact the contact person of the organization or organization directly if the organization does not have a contact person.

Control Reference: 13.c Accounting of Disclosures

Control Specification:	To ensure that disclosures of PII, especially to third-parties, are recorded. To ensure the PII processor notifies the PII controller of any legally binding requests for disclosure of PII. Provisions for the use of subcontractors to process PII should be specified in the contract between the PII processor and the PII controller.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	GDPR Privacy
Level 1 Implementation (example):	PII controllers implement measures that ensure PII processors consult with applicable controllers prior to accepting legally binding requests for the disclosure of PII. PII processers accept any contractually agreed requests for PII disclosure, as long as it is authorized by relevant controllers, unless otherwise prohibited by law. PII controllers disclose that subcontracting is being used and the name of relevant subcontractors, but not business-specific details. The information disclosed will also include the countries in which subcontractors may process data and how subcontractors are obliged to meet or exceed the obligations of the PII processor.

Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P6.2 AICPA Trust Services Criteria - AICPA 2017 P6.7 HIPAA Privacy Rule - 164.504(e)(1)(iii) HIPAA Privacy Rule - 164.528(a)(1)(i) HIPAA Privacy Rule - 164.528(a)(1)(ix) HIPAA Privacy Rule - 164.528(a)(1)(v) HIPAA Privacy Rule - 164.528(a)(1)(vi) HIPAA Privacy Rule - 164.528(a)(1)(vii) HIPAA Privacy Rule - 164.528(a)(1)(viii) HIPAA Privacy Rule - 164.528(a)(3) HIPAA Privacy Rule - 164.528(b)(2)(ii) HIPAA Privacy Rule - 164.528(b)(2)(iii) HIPAA Privacy Rule - 164.528(b)(2)(iv) HIPAA Privacy Rule - 164.528(b)(3)(i) HIPAA Privacy Rule - 164.528(b)(4)(i)(A) HIPAA Privacy Rule - 164.528(b)(4)(i)(B) HIPAA Privacy Rule - 164.528(b)(4)(i)(C) HIPAA Privacy Rule - 164.528(b)(4)(i)(D) HIPAA Privacy Rule - 164.528(b)(4)(i)(E) HIPAA Privacy Rule - 164.528(b)(4)(i)(F) HIPAA Privacy Rule - 164.528(b)(4)(ii) HIPAA Privacy Rule - 164.528(c)(1)(i) HIPAA Privacy Rule - 164.528(d)(1) HIPAA Privacy Rule - 164.528(d)(2) HIPAA Privacy Rule - 164.528(d)(3) NIST SP 800-53 R4 AR-8[P]{1} NIST SP 800-53 R4 AR-8[P]{3} NIST SP 800-53 r5 - PM-21
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization ensures that the development of the strategic organizational privacy plan be done in consultation with the organization’s CIO and CISO, and establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation (example):	The organization develops and maintains an accurate accounting of disclosures of personally identifiable information (PII), including date, nature, purpose of each disclosure, name, and address, or other contact information of the individual or organization to which the disclosure was made. The accounting of disclosures is retained for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer, and made available to the individual to whom the personally identifiable information relates upon request.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	Covered entities provide individuals the right to receive an accounting of disclosures of certain PHI made by the covered entity in the six years prior to the date on which the accounting is requested, except for where restricted by law. An individual’s request for an accounting is: acted upon no later than 60 days after receipt of the request (with a one-time 30-day extension with proper notice to the requester); free of charge for the first request within any 12-month period; and if informed in advance, provided for a reasonable cost-based fee for subsequent requests within the period, as specified by HIPAA § 164.528(c)(1).

Objective Name: 13.02 Individual Participation

Control Objective:	Data subjects are provided a reasonable opportunity and capability to access and review their PII and to challenge its accuracy and completeness.

Control Reference: 13.d Consent

Control Specification:	To make data subjects active participants in the decision-making process regarding the processing of their PII, except as otherwise limited by legislation and regulations, through the exercise of meaningful, informed and freely given consent.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Where feasible and appropriate or where legally required, that PII controller are providing a means for data subjects, or authorized agents, to provide consent before any PII processing begins. PII controllers will ensure that consent adheres to all applicable legal requirements, and is obtained in an informed and transparent manner. PII controllers determine alternate solutions, if necessary, for cases where the practical means chosen are no longer operational, in order to ensure that consent is obtained before any processing begins. PII controllers will store a record of consent. Where feasible and appropriate or where legally required, PII controllers are obtaining consent from data subjects prior to any new uses or disclosures of previously collected PII.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P2.1 HIPAA Privacy Rule - 164.532(c)(2) HIPAA Security Rule - § 164.312(d) NIST SP 800-53 r5 - PT-4 NIST SP 800-53 r5 - PT-4(3) Ontario Personal Health Information Protection Act - 25(2) Ontario Personal Health Information Protection Act - 55.6(2) Ontario Personal Health Information Protection Act - 55.6(5) Singapore Personal Data Protection Act - PDPA 13

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	
Level 2 Implementation (example):	Requirements have been defined for implementing mechanisms to support itemized or tiered consent for specific uses of data.
Level 2 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IP-01(01) (HIGH; MOD) NIST SP 800-53 r5 - PT-4(1) NIST SP 800-53 r5 - PT-4(2)
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The organization is able to demonstrate that the data subject has consented appropriately based on consent. The data subject can withdraw consent at any time and will be notified of this when consenting. Consent is not to be used as a basis for processing if there is a power differential and services are not to be conditional upon consent when PII is not required to deliver the services. The controller takes reasonable efforts to verify that consent is given by the responsible adult if the child is not old enough to provide consent on his/her own.
Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation (example):	A minor child as defined in Texas Civil Practice Code § 129.001 or non-parent of a minor child may consent to medical, dental, psychological, counseling and surgical treatment for the child by a licensed physician or dentist for those circumstances specified in Texas Family Code §§ 32.003 through 32.005. A resident patient may approve or refuse the release of personal and clinical records to any individual outside the facility except as provided in 40 TAC §19.407(3), which states the resident's right to refuse release of personal and clinical records does not apply when: the resident is transferred to another healthcare institution; record release is required by law; or during surveys.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	The elements required for a valid authorization, as specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c), are addressed. The covered entity does not create compound authorizations except when combining authorizations for the same research study with an authorization for the creation or maintenance of a research database or repository, combining authorizations specifically for the use or disclosure of psychotherapy notes, or combining other allowed authorizations, none of which conditions the provision of treatment, payment, enrollment (in a health plan), or eligibility for benefits (but in no case for psychotherapy notes), as specified in HIPAA § 164.508(b)(3).
Level Personal Data Protection Act Implementation Requirements	
Level Personal Data Protection Act Implementation (example):	Data can be collected without consent in certain circumstances outlined in the Second, Third, and Fourth Schedules of the Act. Consent for sending specific messages cannot be required as part of receiving goods or services or based on false or misleading information. Consent is considered given – or deemed – if a reasonable person would believe the use to be directly related to or required to meet the purpose for which consent was given. Consent may also be implied if the data subject provides the personal data voluntarily to the controller. Consent is given to a second organization if the data subject is deemed to have consented to one organization to send it to the other, such as sending information to a bank in response to a purchase including bank routing or a credit card number.

Level CCPA Implementation Requirements	
Level CCPA Implementation (example):	Consumer consent is obtained by third-parties before personal information is sold. Businesses obtain consent from consumers under 16, or from the parent or guardian if the consumer is under 13, before selling personal information.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization develops and posts privacy policies on all external-facing websites, mobile applications, and other digital services, that are written in plain language and organized in a way that is easy to understand and navigate, provide information needed by the public to make an informed decision about whether and how to interact with the organization, and are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization, acting as a health information custodian, determines the capacity of an individual to consent to the collection, use, or disclosure of PHI in accordance with applicable law. If a health information custodian seeks to collect PHI that is subject to a consent directive, the organization, acting as a prescribed organization, notifies the health information custodian that an individual has made a consent directive and ensures that no PHI that is subject to the directive is provided.

Control Reference: 13.e Choice

Control Specification:	To present to data subjects, where appropriate and feasible, the choice not to allow the processing of their PII, to refuse or withdraw consent or to oppose a specific type of processing, and to explain to data subjects the implications of granting or refusing consent.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust EHNAC
Level 1 Implementation (example):	The organization informs individuals in advance of processing, and provides an opportunity to agree to, or prohibit, or restrict the processing of his/her PII. The organization: provides data subjects with the ability to object to specific aspects of the PII processing, rather than data subjects having to accept or object to the PII processing in its entirety; acknowledges the data subject's statement of objection within the time frame specified in applicable laws or as defined in the organization's policy; and will not withhold services from a data subject who declines to provide PII that is not relevant to that service.

Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P2.1 HIPAA Privacy Rule - 164.508(b)(5) HIPAA Privacy Rule - 164.508(c)(2)(i)(A) HIPAA Security Rule - § 164.312(d) Singapore Personal Data Protection Act - PDPA 16
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The organization allows a data subject to object to processing for scientific, historical, or statistical purposes. If the process is necessary for a public interest task, the controller may continue processing the data despite the objection. A data subject may obtain a restriction from a controller where one of the following applies: the accuracy of the PII is contested by the data subject, for a period enabling the controller to verify the accuracy of the PII; the processing is unlawful and the data subject opposes the erasure of the PII and requests the restriction of their use instead; the controller no longer needs the PII for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; OR the data subject has objected to processing necessary for the performance of a task carried out in the public interest, in the exercise of official authority vested in the controller, or for the legitimate interests pursued by the controller or by a third party pending the verification whether the legitimate grounds of the controller override those of the data subject. The data controller ensures that, when processing has been restricted, that further processing other than for storage will only be performed with the data subjects consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State; and informs the data subject prior to lifting such a restriction.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	Requirements have been defined for permitting an individual, or their legally-authorized representative, to request that the organization restrict uses or disclosures of the individuals PII. The organization, acting as a covered entity agrees and complies with requests by individuals for restrictions on disclosure of PHI to a health plan for a healthcare item or service for which someone other than the health plan pays in full, as specified in HIPAA § 164.522(a)(1).
Level Personal Data Protection Act Implementation Requirements	
Level Personal Data Protection Act Implementation (example):	The organization ensures that people may subscribe to have their numbers on the Do Not Call Register or to have it removed therefrom. Withdraw of consent to specific messages may be done at any time, and must be respected.
Level CCPA Implementation Requirements	
Level CCPA Implementation (example):	Consumers who exercise any of their rights are not discriminated against by businesses.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization does not deny any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his or her Social Security number.

Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	In the event an individual's directive to withhold or withdraw the consent to the collection, use and disclosure of their personal health information does not contain sufficient detail to enable the organization to implement the directive with reasonable efforts, the organization offers assistance to individuals in reformulating the directive.

Control Reference: 13.f Principle Access

Control Specification:	To give data subjects the ability to access and review their PII and to challenge its accuracy and completeness.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	CCPA
Level 1 Implementation (example):	The organization publishes a process which governs how data subjects may request access to records maintained in the organization's system. The organization allows data subjects to exercise their right of access in order for him/her to assess its accuracy and to request corrections as necessary (where allowed by applicable legislation). Data subjects will be able to exercise their right of access in a timely manner, without undue cost, in a form understandable and accessible to the data subjects and similar to the means used to collect the PII originally (e.g., by regular mail or by email). Responses to the data subjects regarding this will be provided in accordance with applicable legislation, regulation or as specified in the organization's policy. As practical, responses will be provided in a form requested by the data subject.

Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P4.3 AICPA Trust Services Criteria - AICPA 2017 P5.1 AICPA Trust Services Criteria - AICPA 2017 P5.2 APEC Cross-Border Privacy Rules (CBPR) - APEC VIII 23(b) APEC Cross-Border Privacy Rules (CBPR) - APEC VIII 24 APEC Cross-Border Privacy Rules (CBPR) - APEC VIII 25 CCPA 1798.100(c) CCPA 1798.105(c) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DI-01 (HIGH; MOD) EU GDPR Article 15(4) EU GDPR Article 16 EU GDPR Article 20(4) FTC Red Flags Rule (16 CFR 681) - 681.2c1.ii FTC Red Flags Rule (16 CFR 681) - 681.2e HIPAA Privacy Rule - 164.504(e)(2)(ii)(F) HIPAA Privacy Rule - 164.514(h)(1)(i) HIPAA Privacy Rule - 164.514(h)(1)(ii) HIPAA Privacy Rule - 164.514(h)(2)(i) HIPAA Privacy Rule - 164.514(h)(2)(ii)(A) HIPAA Privacy Rule - 164.514(h)(2)(ii)(B) HIPAA Privacy Rule - 164.514(h)(2)(ii)(C) HIPAA Privacy Rule - 164.514(h)(2)(iii)(A) HIPAA Privacy Rule - 164.524(a)(2)(iv) HIPAA Privacy Rule - 164.524(b)(2)(i)(B) HIPAA Privacy Rule - 164.524(d)(1) HIPAA Privacy Rule - 164.524(d)(3) HIPAA Security Rule - § 164.308(a)(3)(i) HIPAA Security Rule - § 164.308(a)(4)(i) HIPAA Security Rule - § 164.308(a)(4)(ii)(B) ISO/IEC 29100:2011 5.9 NIST Cybersecurity Framework v1.1 - RC.CO-1 NIST SP 800-53 r5 - AC-3(14) NIST SP 800-53 r5 - SI-18(4) NIST SP 800-53 r5 - SI-18(5) Ontario Personal Health Information Protection Act - 53(2) Ontario Personal Health Information Protection Act - 54(1.1) Ontario Personal Health Information Protection Act - 54(2) Ontario Personal Health Information Protection Act - 54(3)(a) Ontario Personal Health Information Protection Act - 54(3)(b) Ontario Personal Health Information Protection Act - 54(9) Singapore Personal Data Protection Act - PDPA 21 Singapore Personal Data Protection Act - PDPA 22 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.345.1 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.346.1

Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	The organization determines the level at which PHI is handled, and then responds to all privacy criteria for access to individual information based on that determination. Level 1: PHI is NEVER directly accessed by any workforce member. Level 2: PHI is sometimes accessible to workforce members. Level 3: PHI is created when workforce members communicate directly with members or patients. Creation of PHI means a designated record check is created. Level 2: Review the HIPAA Privacy Rule Uses and Disclosures regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. Level 2: Review the HIPAA Privacy Rule Individual Rights regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. Level 2: Provide a general statement as to the determination if it is deemed that NO Uses or Disclosures or Individual Rights are deemed applicable. Level 3: Review the HIPAA Privacy Rule Uses and Disclosures regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. Level 3: Review the Privacy Rule Individual Rights regulations and document which requirements apply to your business model and the way in which PHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. Level 3: Provide a general statement as to the determination if it is deemed that CERTAIN Uses or Disclosures or Individual Rights are deemed applicable.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The controller ensures that the data subject has the right to know what safeguards are in place if the data has been transferred outside the EEA. The data controller transmits personal data to another controller, at the request of the data subject.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	If access is denied, the covered entity provides timely (30 days plus no more than a 30 day extension), written denial to an individual's request for access in plain language, the basis for denial, a statement of the individual's rights for review of the denial, a description of procedures for complaints to the entity and the Secretary of Health and Human Services, as specified in HIPAA § 164.524(d)(2). The organization: publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; publishes access procedures in System of Records Notices (SORNs); and adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
Level CCPA Implementation Requirements	
Level CCPA Implementation (example):	The business provides consumers, in response to a verified request, the right to request the categories of personal information collected about them and the actual personal information collected about the consumer. The business provides consumers access to their personal information promptly and free of charge after receiving a verifiable consumer request. The personal information must be delivered via mail or electronically.

Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	An individual's request for access to a record of PHI is acted upon no later than 60 days after receipt of the request (with a one-time 30-day extension with proper notice to the requester, including the reason for the extension) or within the time period specified by the individual (if a basis for urgency is provided and the request is reasonable). The organization, upon granting a request for correction of personal health information, records the correct information in the record, strikes out the incorrect information in a manner that does not obliterate the record or labels the information as incorrect, gives notice to the individual of the correction, and at the request of the individual, gives written notice of the requested correction, to the extent reasonably possible, to the persons to whom the organization has disclosed the information. If it is not possible to record the correct information in the record, the organization informs a person who accesses the record that the information in the record is incorrect and directs the person to the correct information.

Objective Name: 13.03 Purpose Specification

Control Objective:	The authorities which permit the collection of PII and specifically the purpose(s) for which the PII is intended to be used are articulated.

Control Reference: 13.g Purpose Legitimacy

Control Specification:	To ensure that the purpose(s) for processing PII complies with applicable laws and relies on a permissible legal ground.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	HITRUST De-ID Framework Privacy
Level 1 Implementation (example):	The organization determines the legal authority that permits the processing of PII, either generally or in support of a specific program or information system. The organization's purposes for processing PII will comply with applicable law, align with the collector's privacy notice, and rely on a permissible legal basis. Organizations determine whether the proposed PII processing: can be initiated based on a legal ground other than consent (e.g., law enforcement, public safety, legal obligation, or a legitimate interest of the PII controller); is governed by a legal ground that prohibits the data subject from exercising their choice regarding the processing of their PII.

Level 1 Authoritative Source Mapping:	EU GDPR Article 5(1)(a) ISO/IEC 29100:2011 5.3 MARS-E v2.2 - AP-1 NIST SP 800-53 R4 AP-1[P]{0} NIST SP 800-53 R4 UL-2d[P]{0} NIST SP 800-53 r5 - SC-7(24) NY OHIP Moderate-Plus Security Baseline v5.0 - CA-8[PRIV.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PT-2a State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.347.1 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.348.1 State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.349.1
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	Processing relating to criminal convictions or offenses is processed in accordance with EU or member state law or under control of an official authority. The controller limits processing to the six legal bases for processing: consent; contract; compliance with legal obligation; vital interests of a natural person; in the public interest or in the exercise of official authority; or for legitimate interests. Processing that is limited to the scope of the data subject's consent is lawful.
Level Personal Data Protection Act Implementation Requirements	
Level Personal Data Protection Act Implementation (example):	The Do Not Call Registry is being applied to messages offering, advertising, or promoting goods or services address to a Singapore telephone number if the person receiving the call is in Singapore when the message is left or received. The Do Not Call Register is checked before attempting to call or send an applicable message. A person or entity must register to the PDPC to use the Do Not Call Register and update their contact information with the PDPC as necessary. A registered person or entity must apply to the PDPC to determine if a number is on the Do Not Call Register. The message must include the identification of the person or entity sending the message and contact information for the sender. It is assumed that this information will be valid for at least 30 days from the time of the message. Senders of messages may not block their own numbers.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization prohibits the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

Control Reference: 13.h Purpose Specification

Control Specification:	To specify the purposes for which PII are collected no later than at the time of PII collection where feasible and limit the subsequence use to the fulfillment of original purposes.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	

Level 1 Regulatory Factors:	DirectTrust EHNAC
Level 1 Implementation (example):	Where feasible, organizations will communicate to the data subject the purpose(s) of collection before PII is collected or used for the first time for a new purpose. Language which is clear and appropriately adapted to the circumstances will be used. If applicable, sufficient explanations are provided for the need to process sensitive PII. Organizations will regularly review the purpose(s) for which PII is collected to ensure that they are still valid. The organization has identified the specific purposes for which PII is being collected. The purposes are described clearly in the organization's related privacy compliance documentation and/or forms used to collect PII.
Level 1 Authoritative Source Mapping:	ISO/IEC 29100:2011 5.3 NIST SP 800-53 r5 - PT-3 NIST SP 800-53 r5 - PT-5 NY OHIP Moderate-Plus Security Baseline v5.0 - PT-5b Singapore Personal Data Protection Act - PDPA 14(1) Singapore Personal Data Protection Act - PDPA 20(1)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization defines requirements to ensure that all PII must be used for an official government purpose only.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization requests that the individual or individual's authorized representative validate PII during the collection process. The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Objective Name: 13.04 Data Minimization

Control Objective:	Only PII that is directly relevant and necessary to accomplish the specified purpose(s) is collected.

Control Reference: 13.i Collection Limitation

Control Specification:	To limit the collection of PII to that which is within the boundaries of applicable law and strictly necessary for the specified purpose(s).
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Texas Medical Records Privacy Act Privacy

Level 1 Implementation (example):	The organization ensures that the collection of PII is limited strictly to information that is relevant to the purpose(s) of collection and such information will only be obtained by fair and lawful means. Where appropriate, notice will be given to the data subject and/or consent from the data subject will be obtained. The organization is not indiscriminately collecting PII, limits the amount of PII collection from and/or about the data subject from sources other than the data subject, determines which PII needs to be collected to achieve its purpose before proceeding with the PII collection, and refrains from collecting PII which is sensitive, unless the collection of such information is legally authorized, or consent is obtained from the data subject.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P2.1 AICPA Trust Services Criteria - AICPA 2017 P3.1 AICPA Trust Services Criteria - AICPA 2017 P4.1 APEC Cross-Border Privacy Rules (CBPR) - APEC II 18 EU GDPR Article 5(1)(c) EU GDPR Recital 39 ISO/IEC 29100:2011 5.4 NIST SP 800-53 R4 DM-2(1)[P]{1} NIST SP 800-53 r5 - SI-19(1) NY OHIP Moderate-Plus Security Baseline v5.0 - PT-3c NY OHIP Moderate-Plus Security Baseline v5.0 - SI-12(1) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-12(1)[IS.1] OECD Privacy Framework - OECD Part 2 7 Ontario Personal Health Information Protection Act - 11.1 Ontario Personal Health Information Protection Act - 29(a) Ontario Personal Health Information Protection Act - 29(b) Ontario Personal Health Information Protection Act - 55.3(1) Ontario Personal Health Information Protection Act - 55.5(1)(b) Singapore Personal Data Protection Act - PDPA 18
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The organization ensures that personal data is collected only for specific purposes and not processed beyond those purposes unless it is for archiving in the public interest or other select research purposes.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate at an organization-defined frequency but no less than annually.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	Upon receiving notice from a prescribed organization that the PHI collected by the organization, acting as a health information custodian, was disclosed to another health information custodian as a result of one or more scenarios described in PHIPA §§ 55.7(1), 55.7(2), or 55.7(3), the organization will provide written notice of the disclosure to the individual at first reasonable opportunity. If the PHI disclosure was made as a result of the scenario described in PHIPA § 55.7(3), the organization also gives written notice to the Information and Privacy Commissioner in a manner that does not provide identifying information about the individual to whom the information relates or to the group of persons at significant risk of serious bodily harm.

	The organization, acting as a health information custodian, only collects PHI about an individual indirectly if: the individual consents to the collection being made indirectly; the information to be collected is reasonably necessary for providing health care or assisting in providing health care to the individual and it is not reasonably possible to collect, directly from the individual, PHI that can reasonably be relied on as accurate and complete, or in a timely manner; the organization is an institution within the meaning of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act, or is acting as part of such an institution, and the organization is collecting the information for a purpose related to, investigating a breach of an agreement or a contravention or an alleged contravention of the laws of Ontario or Canada, the conduct of a proceeding or a possible proceeding, or the statutory function of the organization; the organization collects the information from a person who is not a health information custodian for the purpose of carrying out research, except if the person is prohibited by law from disclosing the information to the organization; the organization is a prescribed entity and the organization is collecting PHI from a person who is not a health information custodian for the purpose of that subsection; the Commissioner authorizes that the collection be made in a manner other than directly from the individual; the organization collects the information from a person who is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to disclose it to the organization; or subject to the requirements and restrictions, if any, that are prescribed, the organization is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to collect the information indirectly.

Control Reference: 13.j Data Minimization

Control Specification:	To minimize the PII which is processed to what is strictly necessary for the legitimate interest pursued by the PII controller and to limit the disclosure of PII to a minimum number of internal and external parties.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust EHNAC
Level 1 Implementation (example):	Appropriate safeguards are in place for processing related to archiving in the public interest, scientific or historical research, or statistical purposes. Safeguards must ensure data minimization is respected and pseudonymization or anonymization is used when appropriate. Organizations use or offer, wherever possible, as default options, interactions and transactions which do not require the identification of the data subject. Organizations will limit the link-ability of the PII which they collect.
Level 1 Authoritative Source Mapping:	EU GDPR Article 4(5) EU GDPR Article 89(1) EU GDPR Recital 26 Health Industry Cybersecurity Practices - 4.S.B ISO/IEC 27002:2022 - 8(11) ISO/IEC 29100:2011 5.5 NIST SP 800-53 r5 - SI-19(2) Ontario Personal Health Information Protection Act - 44(6)(c)

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Authoritative Source Mapping:	

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Privacy
Level 2 Implementation (example):	The organization, where feasible, uses techniques (e.g., as described in NIST SP 800-122) to minimize the risk to privacy of using PII for research, testing, and training.
Level 2 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DM-03(01) (HIGH; MOD) HITRUST De-ID Framework - De-ID Framework v1 Aggregated Data: Disclosure Policy IRS Pub 1075 - SI-12(2) MARS-E v2.2 - DM-3(1) MARS-E v2.2 - DM-3a MARS-E v2.2 - DM-3b NIST SP 800-53 R4 DM-3(1)[P]{0} NIST SP 800-53 R4 DM-3[P]{0} NIST SP 800-53 r5 - PM-25b NIST SP 800-53 r5 - SA-15(12) NIST SP 800-53 r5 - SI-12(2) NIST SP 800-53 r5 - SI-19(5) NIST SP 800-53 r5 - SI-19(6) NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[PRIV.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25b NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25c NY OHIP Moderate-Plus Security Baseline v5.0 - SA-11[PRIV.1b1] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-12(2) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-12(2)[IS.1] Ontario Personal Health Information Protection Act - 44(6)(c)

Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The organization does not process: PII revealing racial origin; PII revealing ethnic origin; PII revealing political opinions; PII revealing religious or philosophical beliefs; PII revealing trade-union membership; PII revealing genetic or biometric data for the purpose of uniquely identifying an individual; data concerning health; or data concerning an individual's sex life or sexual orientation.

Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	When de-identifying PHI, the organization, acting as a covered entity, requires the removal of all eighteen (18) data elements as required by the HIPAA Administrative Simplification's Privacy Rule, and has no knowledge the resulting data set could be re-identified, or an appropriate person applies generally accepting scientific principles and methods for rendering information not individually identifiable and determines the risk of re-identification is appropriately small. The organization, acting as a covered entity, only creates and uses information that is not individually identifiable (i.e., de-identified) when a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified is not disclosed. If the de-identified information is subsequently re-identified, the organization only uses or discloses such re-identified information as permitted or required for PII in accordance with applicable law, regulation, policy, contract or other relevant obligation.

Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization performs de-identification using validated algorithms and software that is validated to implement the algorithms. The organization performs penetration testing on de-identified datasets to determine if the identified data remains or de-identified data can be re-identified.

Objective Name: 13.05 Use Limitation

Control Objective:	PII is used solely for the purpose(s) specified in the privacy notice and only for a purpose that is compatible with the purpose for which the PII was collected.

Control Reference: 13.k Use and Disclosure

Control Specification:	To limit the use and disclosure of PII for specific, explicit and legitimate purposes and to fulfill the stated purpose(s) or to abide by applicable laws.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust FISMA State of Massachusetts Data Protection Act (201 CMR 17.00) Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) Privacy

Level 1 Implementation (example):	In cases where an employee, contractor or third-party user purchases the organization's equipment or uses their own personal equipment, all relevant information is transferred to the organization and securely erased from the equipment; and, when they have knowledge important to ongoing operations, that information is documented and transferred to the organization. Organizations only use and disclose PII for purposes the data subject has consented to. PII may only be used for purposes beyond that for which it was initially collected if the new purposes are compatible with the original purpose.

Level 1 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(1) AICPA Trust Services Criteria - AICPA 2017 P6.1 APEC Cross-Border Privacy Rules (CBPR) - APEC IV 19 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 AP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IP-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 PS-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 UL-01 (HIGH; MOD) EU GDPR Article 6(4) HIPAA Privacy Rule - 164.502(b)(1) HIPAA Privacy Rule - 164.502(i) HIPAA Privacy Rule - 164.514(d)(1) HIPAA Privacy Rule - 164.514(d)(2)(i)(A) HIPAA Privacy Rule - 164.514(d)(2)(i)(B) HIPAA Privacy Rule - 164.514(d)(2)(ii) HIPAA Privacy Rule - 164.514(d)(3)(i) HIPAA Privacy Rule - 164.514(d)(3)(ii)(A) HIPAA Privacy Rule - 164.514(d)(3)(ii)(B) HIPAA Privacy Rule - 164.514(d)(3)(iii)(A) HIPAA Privacy Rule - 164.514(d)(3)(iii)(B) HIPAA Privacy Rule - 164.514(d)(3)(iii)(C) HIPAA Privacy Rule - 164.514(d)(3)(iii)(D) HIPAA Privacy Rule - 164.514(d)(4)(i) HIPAA Privacy Rule - 164.514(d)(4)(ii) HIPAA Privacy Rule - 164.514(d)(4)(iii)(A) HIPAA Privacy Rule - 164.514(d)(4)(iii)(B) HIPAA Privacy Rule - 164.514(d)(5) HIPAA Privacy Rule - 164.514(e)(1) HIPAA Privacy Rule - 164.530(i)(2)(ii) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) ISO/IEC 27799:2016 8.1.4 ISO/IEC 29100:2011 5.5 ISO/IEC 29100:2011 5.6 MARS-E v2.2 - AC-2a MARS-E v2.2 - UL-1 MARS-E v2.2 - UL-2d NIST SP 800-53 R4 AP-2[P]{0} NIST SP 800-53 r5 - PM-25a NIST SP 800-53 r5 - PT-2 NIST SP 800-53 r5 - PT-3 NY OHIP Moderate-Plus Security Baseline v5.0 - CA-3[PRIV.2] NY OHIP Moderate-Plus Security Baseline v5.0 - CA-8[PRIV.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-21[IS.2] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25[IS.1c] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-25c OECD Privacy Framework - OECD Part 2 10 Ontario Personal Health Information Protection Act - 29(a) Ontario Personal Health Information Protection Act - 29(b) Ontario Personal Health Information Protection Act - 37(1)(g) Ontario Personal Health Information Protection Act - 37(1)(j) Ontario Personal Health Information Protection Act - 42(2) Ontario Personal Health Information Protection Act - 42(3)a Ontario Personal Health Information Protection Act - 43(1)(f) Ontario Personal Health Information Protection Act - 45(6) Ontario Personal Health Information Protection Act - 47(15)(f) Ontario Personal Health Information Protection Act - 48(1) Ontario Personal Health Information Protection Act - 49(3)(a)(i) Ontario Personal Health Information Protection Act - 55.2(3) Ontario Personal Health Information Protection Act - 55.3(2) Ontario Personal Health Information Protection Act - 55.7(4)

Level 1 Authoritative Source Mapping (Cont.):	Ontario Personal Health Information Protection Act - 55.8 State of Massachusetts Data Protection Act (201 CMR 17.00) - 201 CMR 17.03(2)(e)
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	FedRAMP FISMA FTC Red Flags Rule (16 CFR 681) HITRUST De-ID Framework Banking Requirements CMS Minimum Security Requirements (High) Supplemental
Level 2 Implementation (example):	Monitoring the use or disclosure of covered information is required. Such monitoring is supported by automated alerting and response plans. Requirements have been defined, with guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities.
Level 2 Authoritative Source Mapping:	1 TAC 15 390.2 - 1 TAC § 390.2(a)(3) Banking Requirements - FFIEC IS v2016 A.7.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 UL-01 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 UL-02 (HIGH; MOD) HIPAA Privacy Rule - 164.504(e)(2)(ii)(B) HIPAA Privacy Rule - 164.504(f)(2)(iii)(C) HIPAA Security Rule - § 164.312(b) HIPAA Security Rule - § 164.316(b)(2)(iii) HITRUST De-ID Framework - De-ID Framework v1 Audit and Monitoring: Auditing MARS-E v2.2 - SA-11f4 NIST Cybersecurity Framework v1.1 - ID.GV-4 NIST SP 800-53 R4 AU-13(1)[S]{0} NIST SP 800-53 R4 AU-13(2)[S]{0} NIST SP 800-53 R4 AU-13[S]{0} NIST SP 800-53 r5 - AU-13 NIST SP 800-53 r5 - AU-13(1) NIST SP 800-53 r5 - AU-13(2) NIST SP 800-53 r5 - PM-25c NIST SP 800-53 r5 - RA-3c NIST SP 800-53 r5 - RA-3d

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization, at the system or application level, describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy compliance documentation, privacy notices, and privacy policies (e.g., PIAs, SORNs, Privacy Act Statements, and Computer Matching Agreements).
Level De-ID Data Environment Implementation Requirements	
Level De-ID Data Environment Implementation (example):	The organization regularly conducts audits of the use and disclosure of covered information and any identified issues are remediated. The organization only publishes or discloses data that is de-identified for the intended context (environment), unless otherwise permitted by law.
Level EHNAC Implementation Requirements	
Level EHNAC Implementation (example):	The organization ensures all required uses and disclosures of PHI meet the implementation specifications listed in the HIPAA Privacy Rule. Covered entities address the right of access to PHI, accounting of disclosures for PHI, and disclosures of PHI to a personal representative. If the organization is a covered entity, the policies and/or standards related to permitted uses and disclosures of PHI include: Minimum Necessary (required); Extension of Privacy Protection to Deceased Individuals; Authorization to Use or Disclose PHI; De-Identified Information; Limited Data Set; Use and Disclosure of PHI for Purposes of Research; Use or Disclosure of Psychotherapy Notes; Use and Disclosure of PHI for Marketing Purposes; Use and Disclosure of PHI for Fundraising; Use and Disclosure of Genetic Information for Underwriting Purposes; and Uses and Disclosures for Facility Records.
Level Federal Implementation Requirements	
Level Federal Implementation (example):	Requirements have been defined for the disclosure of PHI for a health plan that is a government program providing public benefits and that it only discloses PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits only if the sharing is required or expressly authorized by statute or regulation. Requirements have been defined for, a covered entity that is a government agency administering a government program providing public benefits, disclosing PHI relating to the program to another covered entity that is a government agency administering a government program providing public benefits only if they serve similar populations and the disclosure is necessary to coordinate the functions of such programs.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	Public entities are permitted to transfer data from a public register without the required safeguards as long as not all of the information is transferred and/or if the entity has a legitimate interest in the data. Public entities may only transfer data under a derogation in the public interest, if necessary for a legal claim, if necessary to protect the vital interests of a natural person, or it is made from a public register. Derogations for the public interest relate to public interests expressed in EU or member state law. Assessments made with respect to transfers made under approved derogations must be documented.
Level Group Health Plans Implementation Requirements	
Level Group Health Plans Implementation (example):	The group health plan documents appropriately restrict the use and disclosure of PHI by the plan sponsor, as required by HIPAA § 164.504(f)(1).

	The group health plan documents appropriately limit disclosures to the plan sponsor of information on whether an individual is participating in the plan, or is enrolled in, or is disenrolled from a health insurance issuer or HMO offered by the plan, as required by HIPAA § 164.504(f).
Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation (example):	Individually identifiable immunization information is confidential and may not be disclosed without the written or electronic consent of the individual or the individual's legally authorized representative per Tex. Occupations Code § 159.005. Requests for information from the Texas immunization registry are only made upon the written consent of the individual or, if a child, the parent, managing conservator or legal guardian, or except as provided by the Tex. Occupations Code § 159, or the Tex. Ins. Code § 28B.04.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	If the organization discloses PHI to a family member, or other relative, or a close personal friend of the individual, or any other person identified by the individual, or to assist and locate such a person, the disclosure is limited to that PHI directly relevant to the person's involvement with the individual's care or payment related to such care, or otherwise limited to the requirements for limited uses and disclosures when the individual is not present, for disaster relief purposes, or for a deceased individual, as specified in HIPAA § 164.510(b)(1). The organization only discloses PHI as authorized and to the extent necessary to comply with laws relating to emergency response and disaster relief, as specified in HIPAA § 164.510(b)(4).
Level Personal Data Protection Act Implementation Requirements	
Level Personal Data Protection Act Implementation (example):	Data may only be transferred outside Singapore with adequate protections in place for the data unless the organization has obtained an exemption from the PDPC. Controllers have reasonable security measures in place to prevent unauthorized disclosures and related risks.
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization, when processing Social Security numbers, eliminates unnecessary collection, maintenance, and use of Social Security numbers, explores alternatives to their use as a personal identifier, and informs any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization allows disclosure of relevant PHI to a person conducting an audit, reviewing an application for accreditation, or reviewing an accreditation only if the organization prevents the removal of the disclosed PHI from the organization's facility (unless the removal is authorized by law, or unless the person authorizes the removal and provides that the records will be held in a secure and confidential manner and will be returned when the audit or review is completed).

	If the organization collected PHI on the grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to an individual, a person other than the individual, or a group of persons, the organization does not provide identifying information about individuals or group of persons at significant risk of serious bodily harm in its notice to individuals to whom the information relates.

Control Reference: 13.l Retention and Disposal

Control Specification:	To retain PII no longer than necessary to fulfill the stated purpose(s) or to abide by applicable laws.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust Privacy
Level 1 Implementation (example):	The organization limits the retention of PII to only that which is deemed necessary, limits the retention for as long as necessary to fulfill the organization's specific and legitimate purpose and/or required by law, ensures that retention periods are appropriately followed, and ensures PII is disposed of in accordance with the defined retention periods. Regardless of the method of storage, organizations destroy, erase, dispose, sanitize, and/or anonymize the PII in a manner which prevents PII from being lost, stolen, misused, or accessed without authorization once the PII is no longer needed for the stated purpose for which it was collected and/or at the end of the applicable legally required retention period.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 C1.2 AICPA Trust Services Criteria - AICPA 2017 P3.2 AICPA Trust Services Criteria - AICPA 2017 P4.2 AICPA Trust Services Criteria - AICPA 2017 P4.3 EU GDPR Article 5(1)(e) EU GDPR Recital 39 HIPAA Privacy Rule - 164.504(e)(2)(ii)(J) HIPAA Privacy Rule - 164.504(f)(2)(ii)(I) ISO/IEC 27002:2022 - 8(11) ISO/IEC 29100:2011 5.6 NIST Cybersecurity Framework v1.1 - PR.IP-6 NIST SP 800-53 R4 DM-2(1)[P]{3} NIST SP 800-53 R4 DM-2a[P]{0} NIST SP 800-53 R4 DM-2b[P]{0} NIST SP 800-53 r5 - IA-4(8) NIST SP 800-53 r5 - MP-6 NIST SP 800-53 r5 - SI-12(3) Singapore Personal Data Protection Act - PDPA 25

Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization configures information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a record retention schedule.

Level Group Health Plans Implementation Requirements	
Level Group Health Plans Implementation (example):	Requirements have been defined for subjecting amended plan documents to the organization's retention policy.

Objective Name: 13.06 Data Quality and Integrity

Control Objective:	PII is relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, is accurate, complete and kept up-to-date.

Control Reference: 13.m Accuracy and Quality

Control Specification:	To ensure that the PII processed is accurate, complete, up-to-date, adequate and relevant for the purpose of use.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	To achieve data quality, the organization ensures that PII is accurately processed, complete, up-to-date, adequate, and relevant for the organization's purpose of use. If it is not, it must be erased or edited. Organizations will establish collection guidelines to ensure the quality and accuracy of PII. Upon collection or creation of PII, organizations, where practicable, will confirm the accuracy of the PII, relevance of the PII, and completeness of the PII. Organizations will check applicable programs or systems for inaccurate or outdated PII and correct inaccurate or outdated PII, as necessary.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P1.1 AICPA Trust Services Criteria - AICPA 2017 P6.2 AICPA Trust Services Criteria - AICPA 2017 P7.1 APEC Cross-Border Privacy Rules (CBPR) - APEC VI 21 EU GDPR Article 5(1)(d) ISO/IEC 29100:2011 5.7 NIST SP 800-53 r5 - SC-7(24) OECD Privacy Framework - OECD Part 2 8 Ontario Personal Health Information Protection Act - 55(8) Ontario Personal Health Information Protection Act - 55.2(2)3 Singapore Personal Data Protection Act - PDPA 23 Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(c)

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Privacy
Level 2 Implementation (example):	The organization requests that the individual or individual's authorized representative validate PII during the collection process, and periodically revalidate that PII collected is still accurate at an organization-defined frequency but no less than annually. Requirements have been defined for establishing a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to determine if those agreements comply with the computer matching provisions of the Privacy Act.
Level 2 Authoritative Source Mapping:	CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DI-01(01) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DI-01(02) (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DI-02 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 DI-02(01) (HIGH; MOD) MARS-E v2.2 - DI-1(1) MARS-E v2.2 - DI-1(2) NIST SP 800-53 R4 DI-2(1)[P]{0} NIST SP 800-53 R4 DI-2b[P]{0} NIST SP 800-53 r5 - PM-24a NIST SP 800-53 r5 - PT-8 Veterans Affairs Cybersecurity Program Directive 6500 - b(3)(d)
Level NIST SP 800-53 Implementation Requirements	
Level NIST SP 800-53 Implementation (example):	The organization establishes a Data Integrity Board to conduct an annual review of all matching programs in which the agency has participated.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization ensures disclosed PHI is accurate, complete and up-to-date and notifies the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the disclosed PHI.

Control Reference: 13.n Participation and Redress

Control Specification:	To provide any amendment, correction or removal to PII processors and third-parties to whom personal data had been disclosed.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust CCPA Privacy
Level 1 Implementation (example):	The organization ensures that data subjects have the ability to challenge the accuracy of applicable PII and, where reasonable and appropriate, have the information amended or deleted. PII controllers will establish a process for data subjects to have PII maintained by the PII controller corrected or amended and disseminate corrections or amendments of PII to PII processors and other authorized users of the PII.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P4.3 AICPA Trust Services Criteria - AICPA 2017 P5.2 APEC Cross-Border Privacy Rules (CBPR) - APEC VIII 23(c) CCPA 1798.105(a) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IP-03 (HIGH; MOD) HIPAA Privacy Rule - 164.504(e)(2)(ii)(F) HIPAA Privacy Rule - 164.526(b)(1) MARS-E v2.2 - IP-3a MARS-E v2.2 - IP-3b NIST SP 800-53 R4 IP-3[P]{0} NY OHIP Moderate-Plus Security Baseline v5.0 - PM-22[IS.1d] NY OHIP Moderate-Plus Security Baseline v5.0 - SI-18(4) NY OHIP Moderate-Plus Security Baseline v5.0 - SI-18(4)[IS.1] Ontario Personal Health Information Protection Act - 15(2) Singapore Personal Data Protection Act - PDPA 22(2)(b)
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	When any rectification or erasure of personal data or restriction of processing occurs, the data controller informs the data subject about the recipients to whom the personal data have been disclosed if the data subject requests it. The data subject has the right to have his/her information deleted or erased without undue delay upon request if the data is no longer needed, if consent is withdrawn, if the data subject objects to the processing and there is no overriding legitimate reason to keep it, the information was unlawfully processed, the information must be addressed to comply with an EU or member state law, or if the data was collected from a child by an online entity.
Level Group Health Plans Implementation Requirements	
Level Group Health Plans Implementation (example):	Requirements have been defined for limiting exceptions to the general requirements for amendments to PHI to health benefits provided other than solely through an insurance contract with a health insurance issuer or HMO and PHI that it does not create or receive, except for summary health information or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

Control Reference: 13.o Complaint Management

Control Specification:	To set up efficient internal complaint handling and redress procedures for use by data subjects.
Factor Type:	Organizational

Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	DirectTrust Privacy
Level 1 Implementation (example):	The organization implements an efficient internal complaint management process for data subjects to use. A point of contact will be tasked with receiving and responding to complaints, concerns, or questions from data subjects regarding the organization's privacy practices, policies, and procedures within an organization-defined time period. The organization's complaint management process will provide complaint mechanisms that are easily accessible, are easy to use, and contain all relevant information for filing complaints. The complaint management process includes: tracking mechanisms to ensure complaints are reviewed appropriately; tracking mechanisms to ensure complaints are appropriately addressed within a reasonable timeframe; and corrective actions.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P8.1 CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IP-04 (HIGH; MOD) CMS Acceptable Risk Safeguards (ARS) v3.1 - CMSRs v3.1 IP-04(01) (HIGH; MOD) HIPAA Privacy Rule - 164.526(d)(1)(iv) HIPAA Privacy Rule - 164.530(a)(1)(ii) HIPAA Privacy Rule - 164.530(d)(1) HIPAA Privacy Rule - 164.530(d)(2) HITRUST De-ID Framework - De-ID Framework v1 Complaints: Policy ISO/IEC 29100:2011 5.10 MARS-E v2.2 - IP-4 NIST SP 800-53 R4 IP-4(1)[P]{0} NIST SP 800-53 R4 IP-4[P]{0} NIST SP 800-53 r5 - PM-26 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-26[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-26a NY OHIP Moderate-Plus Security Baseline v5.0 - PM-26b Singapore Personal Data Protection Act - PDPA 12(b)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization acknowledges complaints, concerns, or questions from individuals within 10 working days, completes review of requests within 30 working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time, and responds to any appeal as soon as possible, but no later than 30 working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about privacy practices that includes: all information necessary for successfully filing complaints; tracking mechanisms to ensure all complaints received are reviewed and addressed within 24 hours from timestamp of submission; acknowledgement of receipt of complaints, concerns, or questions from individuals within 24 hours from timestamp of submission; responding initially to complaints, concerns, or questions from individuals within 72 hours from timestamp of receipt of the submission from the requestor; and providing an estimate to the individual of the time when a response can be generated within 72 hours from timestamp of receipt of the submission from the requestor, and keeping the requestor informed at an agreed to time interval for updates, if the initial analysis/response requires more than 72 hours to address the original complaints, concerns, or questions due to the complexity of the inquiry.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	If a requested amendment to a personal health information record is denied, in whole or in part, the organization informs the individual that they are entitled to make a complaint about the refusal to the Information and Privacy Commissioner.

Objective Name: 13.07 Accountability & Auditing

Control Objective:	The organization is accountable for complying with applicable privacy protection requirements.

Control Reference: 13.p Governance

Control Specification:	To establish efficient governance for PII processing.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	The organization develops a comprehensive privacy governance program to ensure the compliance with applicable laws and regulations regarding the processing of PII by programs and systems. The program will be tailored to meet the structure, scale, volume, and sensitivity of the organization's operations and updated periodically. The performance of the program will also be periodically monitored. The organization ensures there is an appointment of a person responsible, such as a data protection officer or privacy officer, who is responsible for the organization's individual privacy protection program. The officer reports directly to the highest management level of the organization (e.g., a CEO). The data protection officer is designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfill required tasks. Data protection officers must be able to act independently.

Level 1 Authoritative Source Mapping:	EU GDPR Article 37(1) EU GDPR Article 37(5) EU GDPR Article 38(2) EU GDPR Article 38(3) EU GDPR Article 38(4) EU GDPR Article 38(5) EU GDPR Article 38(6) EU GDPR Article 39(1) EU GDPR Article 39(2) EU GDPR Article 5(2) EU GDPR Recital 97 ISO/IEC 29100:2011 5.10 NIST SP 800-53 r5 - PL-8a2 NIST SP 800-53 r5 - PM-14 NIST SP 800-53 r5 - PT-7 NIST SP 800-53 r5 - SA-10(7) NIST SP 800-53 r5 - SA-8 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-9a2 NY OHIP Moderate-Plus Security Baseline v5.0 - PT-3d NY OHIP Moderate-Plus Security Baseline v5.0 - PT-7 OECD Privacy Framework - OECD Part 3 15(ii) Ontario Personal Health Information Protection Act - 55.3(14)(i) Singapore Personal Data Protection Act - PDPA 11(3)
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	The controller or their representative maintains adequate records and logs of processing activities. Records or logs of processing are in writing and are available to supervisory authorities. Controllers and processors adequately respond to decisions made by the lead supervisory authority in cases where more than one supervisory authority has jurisdiction. The controller or processor will inform the lead supervisory authority of the actions taken.
Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization, acting as a prescribed organization, ensures practices and procedures for developing and maintaining the electronic health record are approved by the Commissioner. The organization, acting as a prescribed organization, manages and integrates PHI it receives from health information custodians and ensures the proper functioning of the electronic health record by servicing the electronic systems that support the electronic health record.

Control Reference: 13.q Privacy and Impact Assessment

Control Specification:	To establish a privacy impact assessment process and to perform a privacy impact assessment as necessary.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	

Level 1 Regulatory Factors:	Privacy
Level 1 Implementation (example):	The organization conducts privacy impact assessments for systems, programs, or other activities that pose a privacy risk before developing or procuring information technology that collects, maintains, or disseminates PII in an identifiable form. Privacy impact assessments are additionally conducted before initiating a new collection of PII that will be collected, maintained, or disseminated using information technology, and include PII that permits the physical or online contacting of a specific data subject.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P8.1 HIPAA Privacy Rule - 164.530(i)(1) HIPAA Security Rule - § 164.308(a)(1)(ii)(A) HIPAA Security Rule - § 164.310(d)(2)(i) IRS Pub 1075 - RA-3a3 IRS Pub 1075 - RA-8a IRS Pub 1075 - RA-8b1 IRS Pub 1075 - RA-8b2 NIST SP 800-53 R4 AR-4[P]{0} NIST SP 800-53 r5 - CA-2b1 NY OHIP Moderate-Plus Security Baseline v5.0 - CA-2[PRIV.1] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-8a NY OHIP Moderate-Plus Security Baseline v5.0 - RA-8b[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-8b[IS.1b1] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-8b[IS.1b2] NY OHIP Moderate-Plus Security Baseline v5.0 - RA-8b1 NY OHIP Moderate-Plus Security Baseline v5.0 - RA-8b2 Ontario Personal Health Information Protection Act - 55.3(10)(ii)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization reviews the privacy impact assessment (PIA) no less than every 365 days and publishes the PIA.
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	Prior to engaging in a new type of processing or processing using a new system, if there is a high risk involved and a breach occurs, the controller carries out a data protection impact assessment. Processors assist controllers as appropriate with data protection impact assessments and any resulting implementation. If the controller has a data protection officer, the officer is consulted on the data protection impact assessment. Data protection impact assessments are particularly needed if automated processing that will have a legal impact on data subject is occurring, the processing is on a large scale and includes sensitive data, or there is systemic, large-scale monitoring of a public area. If appropriate, a controller consults data subjects or their representatives in developing a data protection impact assessment.

Control Reference: 13.r Privacy Requirements for Contractors and Processors

Control Specification:	To ensure, through contractual or other means, that third party recipients provide at least equivalent levels of PII protection.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	

Level 1 System Factors:	
Level 1 Regulatory Factors:	Privacy
Level 1 Implementation (example):	To ensure that third-party recipients provide adequate levels of privacy, PII controllers will establish PII protection rules and responsibility requirements for the PII processor and document within contracts, either directly or through reference to polices or another agreement, the PII protection requirements that PII processors are required to meet. PII controllers will document and communicate, as appropriate, all related policies, procedures, and practices. Requirements for the use of subcontractors to process PII is specified in the contract between the PII processor and the PII controller. PII controllers and PII processors agree via contractual means that PII is not shared with third-parties without advanced notice, unless specifically permitted in the contract. A confidentiality clause is included, binding both upon the provider and any of its employees with access the PII.
Level 1 Authoritative Source Mapping:	AICPA Trust Services Criteria - AICPA 2017 P6.1 AICPA Trust Services Criteria - AICPA 2017 P6.5 AICPA Trust Services Criteria - AICPA 2017 P6.6 EU GDPR Article 28(3) EU GDPR Article 28(9) HIPAA Security Rule - § 164.308(a)(3)(ii)(B) HIPAA Security Rule - § 164.310(d)(2)(i) ISO/IEC 29100:2011 5.10 MARS-E v2.2 - UL-2b NIST SP 800-53 R4 AR-3a[P]{0} NIST SP 800-53 R4 UL-2b[P]{0}
Level GDPR Implementation Requirements	
Level GDPR Implementation (example):	Processors maintain adequate records and logs of processing activities in which it engages. Controllers are only permitted to use processors who agree to adequately protect personal data. Processors are only permitted to process data pursuant to the instructions of a controller unless required to do so by EU or member state law.
Level HIPAA Implementation Requirements	
Level HIPAA Implementation (example):	The organization, acting as a covered entity, or equivalent, confirms each of its business associates, or equivalents, have a valid agreement that addresses the proper management/oversight of the business associate, or equivalent, specifies applicable requirements (e.g., around use, further disclosure, and the implementation of reasonable and appropriate safeguards), and authorize termination of the contract by the organization, if the organization determines that the business associate, or equivalent, has violated a material term of the contract. In an arrangement between business associate and a subcontractor who handles PHI for the business associate, the contractual requirements apply in the same manner as such requirements apply to contracts or other arrangements between an organization, acting as a covered entity, and the business associate.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation (example):	When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), the following, in consultation with the privacy office, are included in the acquisition contract: a list of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements; privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior; privacy functional requirements, i.e., functional requirements specific to privacy; and Federal Acquisition Regulation (FAR) Clauses per FAR Part 24 (clauses 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act. and Part 39 (clauses 39.105, Privacy, and 39.116, Contract clause), and any other organization-specific privacy clauses.

Control Reference: 13.s Privacy Monitoring and Auditing

Control Specification:	To monitor and audit PII protection controls and the effectiveness of internal PII protection policy.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	PII processing is conducted in a manner which meets data protection and privacy safeguarding requirements. Organizations regularly conduct audits and maintain documentation to demonstrate compliance, and ensure that all audits are conducted by qualified and independent parties, regardless of whether done internally or externally of the organization. If conducting audits with internal resources, organizations periodically have an external party conduct the audit for an independent assessment.
Level 1 Authoritative Source Mapping:	23 NYCRR 500 - 500.03(k) AICPA Trust Services Criteria - AICPA 2017 CC4.1 AICPA Trust Services Criteria - AICPA 2017 P8.1 ISO/IEC 27002:2022 - 5(34) ISO/IEC 29100:2011 5.12 NIST SP 800-53 r5 - RA-8

Control Reference: 13.t Privacy Protection Awareness and Training

Control Specification:	To provide suitable training and awareness concerning PII protection for the personnel of the PII controller who will have access to PII.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	

Level 1 Regulatory Factors:	Privacy
Level 1 Implementation (example):	The organization develops, implements, and maintains a comprehensive privacy protection awareness and training program, organized to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Training is administered at a basic level, at a targeted role-based level, and on a regular basis or as required. The organization will provide guidelines ensuring relevant personnel are kept up-to-date on PII protection responsibilities, developments in regulations that could impact PII or organizational privacy compliance, contracts that could impact PII or organizational privacy compliance, technologies that could impact PII or organizational privacy compliance. Organizations will ensure that after substantial updates, personnel periodically acknowledge and agree to adhere to their responsibilities for PII protection requirements.
Level 1 Authoritative Source Mapping:	Health Industry Cybersecurity Practices - 10.S.A HIPAA Privacy Rule - 164.530(b)(1) HIPAA Privacy Rule - 164.530(b)(2)(i)(A) HIPAA Privacy Rule - 164.530(b)(2)(i)(B) HIPAA Privacy Rule - 164.530(b)(2)(i)(C) HIPAA Privacy Rule - 164.530(b)(2)(ii) HIPAA Privacy Rule - 164.530(i)(2)(i) HIPAA Privacy Rule - 164.530(i)(2)(iii) HIPAA Privacy Rule - 164.530(i)(4)(i)(A) HIPAA Security Rule - § 164.308(a)(5)(i) HIPAA Security Rule - § 164.316(a) ISO/IEC 27002:2022 - 6(3) ISO/IEC 29100:2011 5.10 MARS-E v2.2 - AR-5a MARS-E v2.2 - UL-2c NIST SP 800-53 R4 AR-5[P]{1} NIST SP 800-53 R4 AR-5[P]{2} NIST SP 800-53 R4 UL-2c[P]{0} NIST SP 800-53 r5 - AT-3(5) NIST SP 800-53 r5 - PM-13 NIST SP 800-53 r5 - PM-25d NY OHIP Moderate-Plus Security Baseline v5.0 - PM-13 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-13[IS.1a] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-13[IS.1b] Veterans Affairs Cybersecurity Program Directive 6500 - b(2)(e)
Level CMS Implementation Requirements	
Level CMS Implementation (example):	The organization administers basic privacy training no less often than once every 365 days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every 365 days. The organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every 365 days.
Level CCPA Implementation Requirements	
Level CCPA Implementation (example):	Individuals responsible for handling consumer inquiries are aware of all relevant requirements.

Control Reference: 13.u Privacy Protection Reporting

Control Specification:	To develop, disseminate and update PII protection reports.
Factor Type:	Organizational

Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation (example):	Organizations will promote accountability and transparency in their PII protection operations by utilizing PII compliance reporting as and when appropriate, and external reporting as and when appropriate.
Level 1 Authoritative Source Mapping:	
Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Number of Licensed Beds: Between 200 and 750 Beds Number of Covered Lives: Between 1 million to 7.5 Million Lives Number of transactions received and sent annually: Between 1 and 6 Million Transactions Number of Admitted Patients annually: Between 7.5k and 20k Patients Total Terabytes of Data Held: Between 15 and 60 Terabytes(TB) Volume of Data Exchanged Annually: Between 25 and 100 Megabytes(MB) Number of prescriptions filled annually: Between 10 million to 60 million Prescriptions Number of Physicians on staff: Between 11 and 25 Physicians Number of Patient Encounters Annually: Between 60k to 180k Encounters Number of Individual Records that are processed annually: Between 180k and 725k Records Number of Records that are currently held: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Privacy
Level 2 Implementation (example):	The organization develops, disseminates, and updates reports to: oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates; demonstrate accountability with statutory and regulatory privacy program mandates to privacy officials; and demonstrate accountability with statutory and regulatory privacy program mandates to other personnel with responsibility for monitoring privacy program progress and compliance.
Level 2 Authoritative Source Mapping:	HIPAA Privacy Rule - 164.512(d)(2) NIST SP 800-53 R4 AR-6[P]{0} NIST SP 800-53 r5 - PM-27 NIST SP 800-53 r5 - SI-6(3) NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27[IS.1a1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27[IS.1a2] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27[IS.1b] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27[PRIV.1] NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27a1 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27a2 NY OHIP Moderate-Plus Security Baseline v5.0 - PM-27b Ontario Personal Health Information Protection Act - 55.3(8) Ontario Personal Health Information Protection Act - 55.3(9) State of Nevada Security and Privacy of Personal Information (NRS 603A) - 603A.220.6

Level PHIPA Implementation Requirements	
Level PHIPA Implementation (example):	The organization, acting as a prescribed organization, makes available to the public and health information custodian(s) that provided PHI to the organization a written copy of the results of the risk and privacy assessments carried out by the organization. The organization, acting as a prescribed organization, submits to the Commissioner annually a report containing a record of every instance in which PHI was disclosed since the time of the last report.