HITRUST®

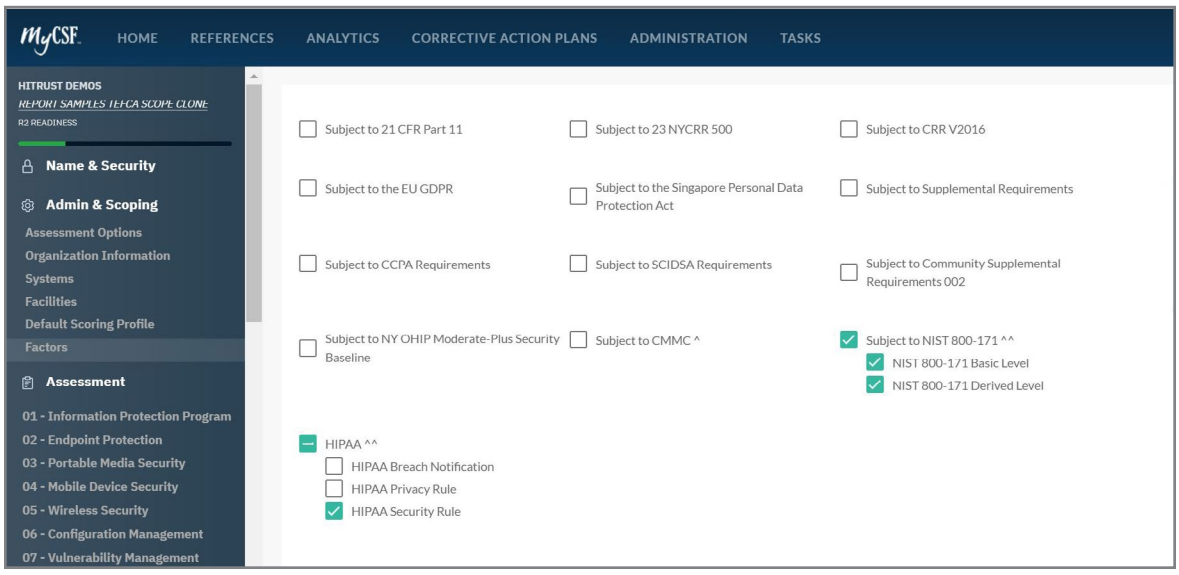
Guide to Tailoring a HITRUST Security Assessment for TEFCA QHIN Applicants

NOTES:

- Based on guidelines in the Common Agreement security requirements, the following guide has been developed to help organizations use a HITRUST r2 Assessment to meet QHIN security requirements.
- Some of the tailoring shown will vary by organization and system.

TEFCA Security Assessment Tailoring and Scoping Selections within the HITRUST MyCSF Platform	
Assessment Options	CSF Security Assessment (mandatory)
CSF Framework Version	HITRUST CSF v9.6.0 or Newer
Organization Type	Healthcare Information Exchange, IT Service Provider, or Non-IT Service Provider
Do you Offer Infrastructure as a Service (IaaS)?	Any Option
Entity Type	Healthcare: Covered Entity, Business Associate, Other (any healthcare option may be appropriate)
Number of Records Currently Held (tied to/assigned to an individual/patient)	Any Option
Geographic Factors	Multi-state or Outside U.S.
Is/Are the System(s) Accessible from the Internet?	Yes (mandatory)
Is/Are the Scoped System(s) (on-premise or cloud-based) Accessible by Third Parties such as Business Partners, Vendors, Cloud Providers?	Any Option
Do the System or Systems Transmit or Receive Data with a Third Party?	Yes
Is/Are the System(s) Publicly Positioned?	Any Option
Number of Interfaces to Other Systems	Any Option
Number of Users of the System(s)	Any Option
Number of Transactions Per Day	QHIN Should Select Max Option
Is any Aspect of the Scoped Environment Hosted in the Cloud?	Any Option
Does the System Allow Users to Access the Scoped Environment from an External Network Not Controlled by the Organization?	Yes
Does the Scoped Environment Allow Dial-up/Dial-in Capabilities (i.e., functional analog modems)?	Any Option
Is Scoped Information Sent and/or Received via Fax Machine (an actual machine, excluding eFax or scan to email)?	Any Option

TEFCA Security Assessment Tailoring and Scoping Selections within the HITRUST MyCSF Platform (continued)	
Do Personnel Travel to Locations the Organization Deems to be of Significant Risk?	Any Option
Are Hardware Tokens Used as an Authentication Method within the Scoped Environment?	Any Option
Are Wireless Access Points in Place at any of the Organization's In-scope Facilities?	Any Option
Does the Organization Perform Information Systems Development (either in-house or outsourced) for any Scoped System, System Service, or System Component?	Any Option
Does the Organization Use any Part of the Scoped System(s), System Components, or System Services to Sell goods and/or Services?	Any Option
Does the Organization Allow the Use of Electronic Signatures to Provide Legally Binding Consent within the Scoped Environment? (including Simple or Basic Electronic Signatures (SES), Advanced Electronic or Digital Signature (AES), or Qualified Advanced Electronic or Digital Signatures (QES))	Any Option
Is Scoped Information Sent by the Organization Using Courier Services, Internal Mail Services, or External Mail Services (such as USPS)?	Any Option
Regulatory Factors	1. Add HIPAA (Security Rule) 2. Add NIST 800-171 (both Basic Level and Derived Level) – per SOP QHIN Security Requirements Section 4.1.b.iii



To find out more about how HITRUST can assist you as a TEFCA resource, we invite you to call: 855-448-7878 or email: sales@hitrustalliance.net.