01 Trust vs. Compliance_David-Houlding_v2.mp3

David Houlding [00:00:03] Compliance is necessary for trust and for health care to be delivered cost effectively and efficiently from a quality of patient care standpoint.

Jeremy Huval [00:00:18] Welcome to Trust Versus, the first episode. I'm Jeremy Huval, innovation officer with HITRUST, and I'm joined by Robert Booker, strategy officer with HITRUST.

Robert Booker [00:00:27] And that voice you just heard at the top of the episode is David Houlding, director of Global Health Care Business Strategy at Microsoft and our guest today.

Jeremy Huval [00:00:34] Yeah, David leads the privacy and security compliance initiatives for Health Care and Life Sciences as part of Microsoft. So clearly the focus of the episode is Trust Versus Compliance, right? But if you have five compliance people in a room, the first thing they'll ask themselves is, "Hey, what kind of compliance do you do?" It's a big field, HR Compliance. Compliance of different legal regulations. We are focusing on information security compliance. It is a subset of organizational risk management and organizational security programs. But it's such an interesting and challenging field and the placement of compliance as the first episode of Trust Versus. I think is reflective of the journey that organizations go through in building out their information security programs from scratch. Atleast a lot of them start by saying, "Look, we have to get compliant with X or Y or Z regulation and we have to adopt this framework to get our customers happy. But it's not the end. It's always the outcome. Robert, how does that strike your ear?

Robert Booker [00:01:36] Yeah, I agree Jeremy. You know, security programs often get started because of a compliance expectation obligation. I need to do HIPAA, I need to do PCI. I need to be compliant with customers expectations. But I think most organizations that have been at this for a while will tell you that they've learned they need to go beyond compliance expectations. Compliance alone doesn't necessarily deliver the secure system they're seeking, and ultimately it's the security of the system that protects the organization, earns it sustains the trust of their stakeholders.

Jeremy Huval [00:02:05] Yeah, so we talk about these topics and more. I'm happy to share this interview with you. Let's kick it off. I'll say in the conversations I've had with you, David, you are uniquely excited about compliance in a way that's sort of it's infectious. And in my career I've spent a whole lot of time talking about compliance with one thing or the other, and it's a unique thing and it's a compliment. I was wondering if you could maybe share a little bit about what keeps you motivated around the topic of compliance and helping others with compliance.

David Houlding [00:02:40] I've always been excited to work in health care. I found the health care industry early in my career. I actually worked in consulting for a stretch and got to try a lot of different industries. Love health care, loved health care the most. Pretty much stayed in health care the rest of my career. Now approaching three decades. And I find that industry very meaningful. And compliance plays such a key role in health care in many different ways. I mean, there's patient treatment plan, compliance as medical device compliance. But more pertinent to this discussion is information, privacy and security compliance. And to me, it's it it's that health care is such a meaningful industry. It's the key role that information privacy and security compliance plays in health care, in helping to establish trust and mitigate risk of adverse events and security incidents like breaches like

ransomware and the things that degrade patient quality of care. In a worst case, could could be a patient safety issues. So to the extent we collaborate on compliance as a tool for health care to help them deliver better health care, better quality of service, quality of patient care, reduce risk of security incidents and so forth. That's what drives me. And I. I get excited about scale, worldwide scale with compliance. So not just the idea of of checking the boxes on some compliance, authoritative source of regulation, data protection or privacy security standard. That's pretty dry. But rather, how can we collaborate together with our partners? You know, health care is such a complex space. And like you, I found health care fairly early in my career and I spent a whole career in health care, information security and privacy as well. And you know, what I find interesting is the the the network effect of health care. I mean, health care is delivered across physicians, hospital systems, payors, governments and in many parts of the world, all working together around the patient and for the benefit of the patient. And as you talk about compliance, enabling health care, I'm just curious about that network effect for compliance. Do you have a thought on that? Yeah. So network effect is really interesting. I mean, in terms of delivering care, there's so many different organizations and even if you just interact with one provider health care entity, there's so many other business associates or data processors behind them that are powering that that care. Right. But there's also the network effect in the sense of, you know, compliance and risk information privacy and security risk. And you can be working with a health care entity and they could have hundreds or thousands of business associates behind them that are adding risk to the equation. And so from a compliance standpoint, how can we ensure adequate privacy, security, information protection, not just for the covered entity, the the data controller, the the the health care provider that you're working with. But but all the entities that they're working with behind the scenes to make sure that there isn't a weak link or the weak link in the chain is sufficiently strong enough that, you know, we mitigate the risk of breaches, ransomware and that kind of thing to an acceptable level.

Jeremy Huval [00:05:44] You know, I'm to go back to even more basic question, like, does compliance itself make organizations more secure? What's the value? How does it really help?

David Houlding [00:05:53] So in terms of establishing a common standard to ensure adequacy of privacy security controls, I think the risk of not having compliance to an authoritative source of regulation of data protection on information, privacy and security standard. The risk of not having that is people resort to sort of ad hoc techniques like questionnaires and whether those questionnaires sufficiently mitigate risk or recognize risk to confidentiality, integrity, availability of of health care data. You know, that's that's really a big question mark. And it really depends on who created that questionnaire. And there's such wide variability across organizations. So I think the real value of compliance is establishing that common bar that that common standard of adequacy and and having mutual trust in that standard that, you know, say I'm a business associate or data processor, I deliver some service I can present to a covered entity like a health care provider and say, "Hey, I meet the same standard that you recognized." And we know that that is a common trusted standard that both organizations respect and know is a is is meets and in many cases exceeds the needed levels of information, privacy and security. That trust can be established very quickly and enable business enable health care. To me, you know, compliance is about foundational layer of health care that compliance serves health care, not the other way around.

Jeremy Huval [00:07:27] David said something kind of interesting, "Without regulators and really without standards or frameworks, there's no common source of establishing the bar necessary that we would all share the bar of compliance."

Robert Booker [00:07:41] Right. Almost like a common trusted standard. David also had a quote that said, "The risk of not having compliance to an authoritative source is the risk of having people resort to ad hoc techniques." So there's something there in both of those quotes.

Jeremy Huval [00:07:55] Yeah, I think there is, so compliance in my mind has value in that It establishes the common expectation of what we're all supposed to be doing. And meaningful compliance is accompanying by assurance. Right? So it's one thing to have a list of to do items, but if there's not the assurance that I can use to communicate, hey, not only am I meeting these things, but I can prove to you that I'm meeting these things in a way that gives confidence that, hey, I'm not just saying it because I want I know you want to hear it. And compliance is valuable to me too, because it allows organizations to examine themselves and to be examined around their performance of certain things that are so critical to protecting information, for example, in the context information security compliance.

Robert Booker [00:08:40] Yeah, well, it's really almost just in the proof, isn't it? I mean, how do I prove how do I know what level of confidence can I speak to, around my compliance outcomes? And I think the assurance that you mention is what drives that and also gets to the organization being able to establish trust with the people that that matter. I mean, I think about internal trust with executive leaders and companies, board of directors, you know, them knowing that the program has a level of rigor and assurance around it that the compliance is actually achieved and can be proven, but also customers, regulators outside the company, those people that, you know, write the laws and standards that we all have to meet. You know, being able to prove to them, too, that we have a compliance program that has a high level of assurance, I think that's really just key to all of it.

Jeremy Huval [00:09:25] Yeah, and it's interesting to hear David's perspective because his focus is not only compliance on domestic stuff, but also global compliance scale. And I like what he said about staying motivated around compliance. And I really like the question around, "Does compliance make us more secure?" So with that said, let's get back into it.

Robert Booker [00:09:45] Let's go. You know, compliance requires a level of confidence. The word we would use is assurance, and then assurance requires an audit or some form of validation, which I really think about audits to assurance, to compliance, to, you know, does the audit itself make us secure, or is that just a tool to get to compliance?

David Houlding [00:10:08] I think it's it's a very important tool in the enforcement of compliance. It sort of depends on the authoritative source, right. If it's a voluntary, authoritative source that many, many different health and life sciences organizations, then you know, they're going to undertake the audit and getting audit ready, getting assessed, getting certified, right. But then you get other types of authoritative sources like HIPAA, which is a government regulation by the Health and Human Services enforced by the OCR Office of Civil Rights. Even though given organizations should comply with HIPAA, whether they do or not. Unfortunately, maybe they don't. If there isn't any sort of random audits happening, you know, identify risks that are above the baseline of acceptable risk, you know, do what they need to do to mitigate those risks to a sufficient level of residual

risk. And again, make sure that everybody is adequately secured and health care can thrive.

Jeremy Huval [00:11:05] Can you talk a little bit about what surprised you the most, maybe as you started to understand the different bars that these different governments have set by way of this is what we think, this is what we think this is what we think.

David Houlding [00:11:18] And how they come to be is so different, right? Like often the sort of regulations in the U.S. are sort of in reaction to some harm like breaches have occurred. We don't want that but many of them come about from the standpoint of, you know, individual rights, like the rights of the data subject, the rights of the patient, right. Like data protection laws typically follow that, and they're sort of based on government sort of policy and that kind of thing. And then you get information, privacy and security standards like the ISO 27,000 series, which are striving to define that common level of privacy security worldwide. Right? And set that adequacy level across, you know, all countries worldwide. So the sort of where they come to be is so different. I mean, as you go across countries, you go across jurisdictions. So you could have regions like Europe, which is, you know, GDPR. You can have countries like the U.S., which is you could have even state level or province or territorial level, you know, authoritative sources like CCPA in California or Ontario PHIPA in Canada, province of Ontario. The reason that's so interesting is if you're a very large organization like Microsoft with a platform like Azure, which literally has worldwide reach, you know, Azure is independently certified against literally over 100 different compliance frameworks. I trust this one HIPAA's another and, you know, independently sort of audited and assessed and certified against each one. But there's not many organizations in the world or solutions in the world that can do that. It's just too expensive.

Jeremy Huval [00:12:55] If I think about overlaying cloud on top of that, for organizations that are entering the cloud and transferring their legacy systems into cloud, what tips would you give them? What would you say as a must do when you're working on figuring out how do I how do I get this right and not drop the ball by way of compliance as I transition into the cloud?

David Houlding [00:13:18] If I'm a health care provider, I'm held to HIPAA, and that's regardless of whether I'm doing cloud or not. Right? And so I could be all on prem with my servers, on premise servers and so forth, my own data center. And then I decide, okay, I'm going to make use of a cloud, whether it's Microsoft Azure or some other cloud and or maybe it's multi-cloud, right? And so I'm embarking on that journey to cloud, because cloud is not I'd like one day I'm on prem, the next day I'm in the cloud. Cloud is like a journey, right? And it could take organizations even years to get a single workload in the cloud. Like they might decide we're going to move our electronic health record system to the cloud, and that typically could take over a year. And compliance needs to be maintained from the on prem through that journey. And then on the cloud ongoing. And during that journey, you've got a hybrid, right? You could have some workload, some elements of your EHR workload on prem and your productions, Jeremy, the last to go to the cloud, other environments could already be in the cloud. You still got to be compliant right during that phase. And then once everything gets in the cloud, you've got to be compliant, ongoing in the cloud. So that that's a challenge. And one of the really cool things with the cloud is this notion of shared responsibilities and inheritance. If you were all on prem, you have to do all those requirements yourself, right? But if you go into the cloud, you can lean on the cloud provider through shared responsibilities and inheritance to to meet those physical security requirements.

Jeremy Huval [00:14:47] So just a debrief on that one. We talked a lot about some privacy focused regulations. I mentioned earlier, we're talking about information security. Really opening up the aperture to information protection to include privacy. That's when you start to bring in PHIPA in Ontario, which is their health care regulation. You got GDPR in the EU, which is so privacy focused, and we know that we can't have security without privacy. So I'm really glad that we brought that into the conversation. Robert, how do companies earn trusts and consider rights like, you know, the rights of individuals that are protected by these privacy regulations alongside all the different regulatory requirements they have to focus on?

Robert Booker [00:15:29] Yeah, I think you said it well, Jeremy, it's really the what versus the how. I mean, privacy is what we're achieving, protecting the individual rights of the people and the information that we serve, the How we do it, is the information security framework around it and the overall compliance of both work together. I don't think you have privacy without security. You certainly shouldn't deliver security without a mind to the business problem you're solving, which is privacy. I think you have to think about them together.

Jeremy Huval [00:15:54] Yeah, and that's maybe a bit not fair because so much of the media headlines go toward the latest security problem, the latest security breach. But a lot of these security efforts underpin the need to protect data and protect individual rights and protect personal records from being shared inappropriately at all times together as part of a common ecosystem that where one depends on the other.

Robert Booker [00:16:19] I think that we we have to go back to the basics again. So all new threats are mitigated by security controls. So we think of this as all new things, but they're really not new. I mean, vulnerabilities and purchase software became new two to three years ago, but it's resolved by keeping your software up to date once those vulnerabilities are resolved. So they're all they're all worthy and foundational, regular testing and assurance. And without those, you do have these issues that result in what is what is called today a privacy breach.

Jeremy Huval [00:16:45] I also like how David mentioned moving to the cloud is a journey. It's a long term journey for a lot of organizations. That's true of compliance as well. Achieving your compliance goals and and largely that's true of achieving your information security goals as well.

Robert Booker [00:17:01] I mean, compliance is never done, even though we we look at this as a series of assurance steps or audit steps or validation steps, but it's really about the system and the system being continuously validated and the system being continuously updated.

Jeremy Huval [00:17:15] Absolutely. It's exciting time for change, too. I think about all the new technologies that are becoming more and more accessible to businesses large and small, like AI and blockchain. And, you know, there's there's risks associated with adopting any new technology, especially these. And I think about what's coming in terms of the compliance landscape and how it will change to address, you know, these emerging technologies.

Robert Booker [00:17:39] Compliance is going to have to keep up and compliance is going to have to evolve as the technology evolves. Like David touches on that a little bit more let him break it down for us.

David Houlding [00:17:50] Things are moving faster and faster. There's really exciting changes like A.I., but blockchain, many others that are essentially bringing are promising some very compelling new benefits, including to health care and the quality of care and, you know, basically empowering health care professionals to make better decisions faster and proof quality of care, lower cost of care, that kind of thing. So really exciting. But these these new technologies, like any technology, can be a double edged sword. It can be used nefariously as well as for good. And A.I. is no exception. And you know, it can be used in things like phishing and spear phishing and deepfakes, whether audio or video, etc.. And so as a cybersecurity compliance professionals, I think we all need to be thinking about how can we ensure that we enable the good, maximize the good and minimize the risk of the bad. The interesting thing is because I mean, very often I know I'm preaching to the choir here, but very often there's a lag time between compliance and controls and requirements within a given compliance sort of authoritative source and where the industry actually is in terms of, you know, IT landscape, like as it's shifting from on prem to the cloud, is are there new risks from AI and so forth. Very often there's a lag time. Is it six months, is it multiple years for the regulations and so forth to catch up with, hey, this this new technology or the shift as introduces new vulnerabilities and new risks? So I'm really excited about some of the cyber adaptive stuff that's happening at HITRUST and, you know, tracking those kinds of shifts much more closely on a like monthly basis and and being able to to deliver new intelligence and updates to organizations that are high trust licenses in terms of helping them see what they need to change in their what controls are they complying with are getting in place.

Jeremy Huval [00:19:47] I've heard you talk many times about leading with compliance as a winning strategy. Can you talk about how compliance can be a competitive advantage? I think oftentimes people think about compliance as this burden, this ball and chain that they have to drag behind them as they enter new markets and and take on new types of data. But how do you change the thinking? How can compliance be the thing that helps us as opposed to burdens us?

David Houlding [00:20:14] Confusion about compliance can impede solution adoption. So health care needs a given solution to render better care, more cost effective care, whatever the case may be. They need a solution, but they're concerned about compliance and therefore it impedes or in some cases blocks the adoption of said solution and the realization of the value of that solution. So by leading with compliance, what what we are doing is really getting ahead of that, and it's very central to the role I have at Microsoft, where I'm going beyond what Microsoft does for its own certifications of its own platforms, so we can bring that clarity to health care organizations to alleviate that confusion, remove the impediment to the solution adoption, accelerate adoption of said solution, and then furthermore, get them focused on their responsibilities, like what are the gaps of their responsibilities and achieving the full compliance. And so we're really excited about that. And that's that's what we think about when we talk about leading with compliance. Now, that's not to say that compliance is always sufficient in and of itself, and we talked about the relationship of risk management and compliance and sometimes interestingly, the compliance framework, like if you're talking about even HIPAA, for example, requires risk analysis to be done. So, you know, very, very often hand in hand, sometimes risk analysis is going above and beyond or specializing in various ways, but we do tend to lead with compliance and then address other things as needed, like, hey, this particular customer's

really concerned about ransomware or distributed denial of service, how they model that risk, what can we add to further mitigate that risk if needed is kind of how we think about it. We've talked so much about the positives. So can you think of incidents or, you know, industry trends where things didn't go like we'd like and compliance and regulation became more of a priority as a result? Yeah, unfortunately. I mean, compliance can be a proactive thing, but so often it's a reactive thing and it can occur as a result of some incident that's occurred like a breach or ransomware and the disruption and the negative consequences. So I think too often that happens with organizations either not not complying with what they need to comply with or not complying with enough for a sufficiently a sufficiently high level of compliance like maybe they were just HIPAA before, but they really needed to be HITRUST to sufficiently mitigate risk. And, you know, because they weren't they had a breach or some adverse event that very often impacts the in-patients. Right? So to the extent we can all be more proactive about information, privacy and security and compliance is a big part of that, as is risk management. We can mitigate risk of those those things faster, sooner and reduce that window of opportunity for adverse outcomes of security incidents like like breaches and ransomware.

Jeremy Huval [00:23:12] So we'd like to thank David Houlding for his time and expertise, and we hope everyone listening found this as informative as we did. One of my big takeaways from that part of the conversation was confusion about compliance can impede solution adoption. So Robert, I've been working on compliance a long time and I never really had that aha moment. And I'm embarrassed to say I should have because I've helped organizations implement different technologies and help them answer the question of what do I do to comply with, say, HIPAA over this new EMR or what have you. But it makes sense. David's role at Microsoft is to help everyone understand just how equipped an organization like Microsoft is, is to comply with different regulatory needs and different markets at a global scale. Confusion about compliance can impede solution adoption, and that, to me, you know, it makes sense. It's so important to have clarity and an understanding and sort of an easy button for answering these kind of compliance questions. What do I need to do to protect my data in a manner that will keep me out of hot water while also mitigating risks to the level they need to be mitigated? What were some of your key takeaways?

Robert Booker [00:24:24] I think the way we think about compliance between organizations and, you know, if we think about compliance as a requirement to follow, I actually wonder about compliance as a tool to allow for organizations to share between each other how they're doing their obligations. So keeping their clients, keeping their customers, keeping their employees safe if we're talking about trust and trust versus compliance. Ultimately, the compliance leads to the trust. And so having having an out system that allows you to reflect on all that is really important.

Jeremy Huval [00:24:55] Yeah. And maintaining a high level of assurance is important as well. It's very different to try to meet the bare minimum of compliance standards and sort of a passive way after the project is done and everybody goes home and says, "Congratulations". That's very different than actively practicing compliance and taking that next step to achieve assurances to communicate to your stakeholders. Not only were doing this, I can prove it to you and you can have confidence in the messaging and confidence and the actual procedures and assessment evidence that was collected behind my assertion that, yes, we are compliant. No, you don't need to worry about, you know, us when you give us data as you know, as your as your vendor, for example, audits and assessments can be an important way of making sure your organization is meeting those satisfactory standards of trust and level of assurance that's necessary.

Robert Booker [00:25:52] Yes, and expecting compliance to be a part of the program, but not the whole goal of the program is key because we're talking about compliance as a as an outcome, as a proof of assurance, as a proof of trust. But staying ahead of developments with threats and using compliance and assurances tools to help maintain that system and keep that system healthy and operating with the right level of maturity is super important to the organizations you work with and to how you communicate internally.

Jeremy Huval [00:26:19] Yeah, and the advancements and technology will see the compliance standards and regulations and frameworks try to keep up. You know, there's an interesting lag between, you know, the introduction of new tech, the adoption of new tech and the following of compliance standards, regulations and control frameworks. There's a lot of change going on. And like we mentioned, AI that was a cool part of the conversation. I'm looking forward to things to come.

Robert Booker [00:26:48] So with that, I want to thank all of you for listening to us today. Trust versus Presented by HITRUST. We're challenging trust in discussions across the world of security, compliance and assurance. We hope you join us again on our journey. Thanks for being with us.