HITRUST's Evolution and Important Role in Strengthening HIPAA

Excerpts from HITRUST and Cybersecurity 2018: Part 1- Evolution and Adoption

As recently announced, Evolve IP is proud to have achieved the honor of being HITRUST CSF certified. View the HITRUST certification press release here. Certification to the HITRUST Common Security Framework (CSF) affirms that all of Evolve IP's cloud computing and cloud communications services adhere to the strictest security standards for electronic protected health information (PHI). The reason that HITRUST is a critical component of today's healthcare conversation is that it focuses on the most important issue facing the industry today: data security. Our 250+ healthcare clients have always received HIPAA compliant cloud services. But HITRUST is in a different class.

HIPAA compliance is certainly very important, but being "compliant" is far different from "providing a culture of data security". That's the difference that HITRUST makes.

To help our clients and all participants in the healthcare community (ranging from covered entities as well as any service providers who touch PHI data) understand the implications of HITRUST, Evolve IP recently hosted a seminar entitled HITRUST and Cybersecurity 2018. The day's first keynote speaker was Omar Khawaja, the Chief Information Security Officer (CISO) at Highmark Inc. in Pittsburgh. Below are some excerpts from his keynote address (47 minute video clip) that explain how HITRUST changes the game. Specifically, the excerpts answer the following questions:

- What problem were you trying to solve when you began thinking about HITRUST?
- Why is HITRUST a great fit for the security demands of healthcare?
- How did you decide to start requiring HITRUST certification for your vendors?
- How and why is support for HITRUST growing?

- Are your third parties complying with the HITRUST requirement?

What problem were you trying to solve when you began thinking about HITRUST?

I realized that the amount of risk posed by our information that was (being held by business associates) outside of our four walls was significantly greater than the risk posed by what is inside our four walls. That's simply because of the math. We've got probably 10, or 20, or 30 times more of our members' information that we are sharing with some third party through the course of doing business than that which actually exists within our own four walls. So it's important for us to have a good security program at Highmark Health, but it's probably MORE important for us to have a phenomenal strategy for ensuring that our members' information, and our patients' information, is just as secure when it leaves our four walls.

We run eight hospitals with about 400 physician offices. We also provide medical vision and dental insurance to customers all over the country. All told we have about 45 million customers across the country who were responsible for. Protecting their information is the thing that keeps me up at night because that is that is my responsibility.

Why is HITRUST a great fit for the security demands of healthcare?

The HITRUST CSF is a risk-based control framework and it actually maps to 20 different compliance requirements and authoritative documents (2 minute video clip). If you're concerned with PCI, HIPAA/HITECH, various state privacy laws, ISO 27001, NIST, FFIEC requirements and probably about 8 or 10 others, HITRUST essentially harmonizes them. It doesn't come up with something new, it just takes a lot of those existing compliance requirements and build crosswalks against them.

In order to achieve the HITRUST certification an approved CSF assessor must validate every single control. Further, the recertification happens every two years and upkeep of the control framework is every single year. Consistently, HITRUST has updated the common security framework based on feedback from the industry from the auditors from the assessors and from the government. So it does evolve based on the needs of the industry.

How did you decide to start requiring HITRUST certification for your vendors?

In early 2016 Highmark got together with four other healthcare payers – HCSC, UnitedHealthcare Group, Anthem and Humana – to agree on an approach, because if we do something individually it's probably not going to be as effective as if we do something as a group. We all decided on three things:

- We're going to have our control requirements defined by the HITRUST Common Security Framework (CSF)
- Controls must be validated by an approved HITRUST assessor, and
- Our business associates must obtain a HITRUST CSF certification within two years (2018)

In our approach, five large health plans partner together to convey consistent and easy-to-understand requirements. Among us we actually had 7500 third parties that this requirement went out to. The requirement is easy. You just have to go get HITRUST certified (1 minute video clip). The requirements get updated every year. Every two years you have to go get recertified. We don't have to update our contracts every year just because there's a new cyber threat out there.

The number one thing I was looking for is that 100% of my third parties have an evidential review of policies and validation of every single security control. I just want 100% of my vendors to be HITRUST certified. Otherwise I don't feel comfortable going to my customers and saying "trust us, we're on it."

How and why is support for HITRUST growing?

- At this point there's probably close to 90 or a hundred organizations out there that have done the same thing that the five of us did to begin with: they have now required all of their third parties to be HITRUST certified.
- Organizations are convinced that HITRUST is here to stay (38 seconds). I can tell you that because I'm now starting to see a lot of demand and growth from the financial services industry. And I'm starting to see it from the technology sector. And for other areas where they aren't in healthcare. They don't have protected health information (PHI) but they're looking at this framework and saying "this is what we want to do" and "this is what we're going to use.
- Today we're seeing it work because organizations are seeing value (35 seconds). In just the month of September my team had three questionnaires that we were able to go back to our customers and say "hey, we've got this HITRUST certification. Do you really want us to respond to your questionnaire or would you like the three hundred page report from HITRUST based on an on-site audit that lasted three months. In all three of those cases they said "forget about the questionnaire, just send us the report." That is value right there.

Are your third parties complying with the HITRUST requirement?

To date the vast majority of our third parties see the value in the approach and have committed to it. There's one vendor that was escalated to me and I had to have about two or three conversations with them to say "why aren't you getting HITRUST certified? And if you really aren't, let me know because then we need to start making plans to stop doing business with you." Because we were serious. They came back to me in spring of this year and said they are going to go and get HITRUST certified.

I was talking to one of the Fortune 10 technology vendors earlier this year and they said "we have certification A and we have certification B and we have this in terms of our certifications" and I said "but none of them work for healthcare. This (HITRUST) is what you need to do for healthcare (43 seconds). What you're doing doesn't really work for me in healthcare. Give me something that works for me. It's okay if you don't want to serve the healthcare industry. We can go to a different vendor. But I can tell you that this is the expectation within healthcare.

Contact us today for more information about Evolve IP's HITRUST certified communications and computing solutions, or about our upcoming educational events.