Exploring Encryption and Standards in Release of Information

Save to myBoK

By Mary Butler

The HIM Problem

As providers and business associates bring themselves into compliance with the HITECH-HIPAA Final Rule, encrypting data in transmission and at rest can pose a challenge. Two ROI experts discuss encryption and the use of standards in privacy and security.

HIM Problem Solvers

Scott Ruthe, CSSP, CBCP, VP of network and security, HealthPort
Paul Gue, CIO, HealthPort

Journal: What can providers and business associates (BAs) that handle PHI be doing to prevent a breach and comply with HITECH-HIPAA?

Gue: I think based on HIPAA rules and regulations, encryption of any kind of data in transit is a requirement. We encrypt any data we're sending from our resources or our representatives in the field who are getting release of information (ROI) information from our data center. The data we send out to our requestors in transit is definitely encrypted. What's not required today—but is strongly suggested, and I think a lot of companies haven't done—is encrypting the data at rest.

Ruthe: The other point we want to make is encryption is one piece of the puzzle, part of those layers of security. Encryption is one way to prevent that loss but another method we use is software that allows us to remote block and remote wipe a PC. So not only is it encrypted, but we can also issue a command if we know that a PC has been lost. Any time it touches the Internet after that, it will then block that PC so it is useless to the thief.

What are some barriers to encrypting data at rest?

Ruthe: There is a fairly significant cost depending on the size of data that you're storing. It's definitely a large cost. There's also somewhat of a performance hit because every time a system accesses encrypted data, it has to decrypt and then re-encrypt after it's finished using that data. So there's a lot of system impact as well—definitely not a trivial implementation to get encryption of your internal data at rest completed. It's becoming one of those necessary requirements to make sure that you're protecting your client's data and the data you're holding.

What types of vendors and providers are less likely to encrypt data at rest?

Ruthe: What we've seen mostly is smaller companies. So if you have someone that's say, a small doctor's office, like a family of doctors or a small dental practice, small practitioners. They won't be doing the encryption because they're just not big enough to absorb that.

What are some privacy and security tasks that require technical standards?

Ruthe: Let's look at it from an architecture point of view. We have an architecture security team that reviews all of the installations to ensure we're in compliance with the technical standards that are being required. Whenever we're bringing in an upgrade or new patch or new system, or anything like that, it gets reviewed prior to installation. It validates security from a technical standpoint.

We also go through on an annual basis and perform a risk assessment (as required under HITECH) where we review all the systems in place to ensure they're still meeting the compliance we already set and look at the new legal guidelines coming out and not missing anything that's been announced that we now need to comply with.

Gue: Probably one of the biggest holes that we see in the provider world is a complete risk assessment that's completed on an annual basis. Systems change all the time and that risk assessment is critical to systems you have in place. The risk assessment is a time consuming process.

Which standards do you recommend using?

Ruthe: We use NIST (National Institute of Standards and Technology as our primary base since that's the Office for Civil Rights (OCR) requirement, and we've started using HITECH-HITRUST standards to meet industry guidelines.

Gue: NIST and HITECH are two of our primary. When we do stock audits we go through annual penetration tests, that requires a lot of external validation of our controls, but the base guideline is driven by NIST standards and HIPAA and HITECH.

Mary Butler is the associate editor at The Journal of AHIMA.

Original source:
Butler, Mary. "Exploring Encryption and Standards in Release of Information" (Journal of AHIMA website), January 2016.
