Haekka

Lesson 14 | HIPAA and Technology

Updated 2020-09-12

HIPAA and Technology

HIPAA is not new. It was written before there was a “cloud”. Also, the organizations that need to comply with HIPAA in 2020 are incredibly broad, which is why HIPAA can be frustratingly vague.

Increasingly, incumbents and new entrants into healthcare are using modern technology. As healthcare modernizes its technology stack, it is dragging HIPAA along for the ride.

When it comes to software development in any regulated industry, both security and privacy need to be a part of the system development life cycle (SDLC). Privacy reviews should be a part of feature documentation before any software is actually written. Then there should be a privacy signoff before features are put into a production product. These reviews and signoffs should be documented.

The other major technology area where there remains confusion and ambiguity is the cloud. The major cloud providers are, in this order, 1) Amazon Web Services (AWS), 2) Microsoft Azure and 3) Google Cloud Platform (GCP). The cloud has ushered in a new term - *HIPAA Eligible*. The cloud providers have 100s of cloud services. Some, but not all of those cloud services are *HIPAA eligible*. This basically means that the cloud providers will sign a BAA with you if you want to use these *HIPAA eligible* services for PHI. *HIPAA eligible* does not mean the cloud service is configured in a way that complies with the HIPAA Security Rule, doing that is up to the cloud customer.

The cloud is just a new form of technology and, as such, you should follow similar procedures to any other form of technology being utilized under HIPAA, namely following a SDLC with privacy and security as a component.