COSMOS
Navigate the Compliance Universe

Compliance Today - February 2019
OCR's Cyber Security Newsletters: "Cheat sheets" for good security compliance in our cyber age

By Iliana L. Peters, JD, LLM, CISSP

Iliana L. Peters (IPeters@Polsinelli.com) is a Shareholder in the Washington, DC offices of Polsinelli, PC.

Most businesses, whatever the economic sector, acknowledge that they must devote resources to understanding and implementing data security, particularly given that security incidents and their fallout make the news on a daily, if not hourly, basis. Conversations about risks for data security breaches happen at breakfast tables and boardroom tables around the country, and topics range from social media to national elections to international espionage. For compliance personnel, these conversations boil down to concrete reasons for investing the resources in implementing data security practices and the best ways to do so. Importantly, good data security in our current cyber age is essential for entities of all sizes, types, and focus areas, for a few very persuasive reasons, including:

- An entity's data is its most valuable asset, replacing assets that used to be considered more high-value, from physical assets to copyrighted material to well-trained employees, in a corporate valuation analysis.[1]
- An entity's reputation is on the line anytime its data is compromised in a data breach or cyberattack; recent examples of high-profile data breaches have angered both consumers and state, federal, and international legislators and regulators.
- Good data security is required under state, federal, and international law, and violations of these laws can have serious penalties.
- With respect to certain critical economic sectors, such as the healthcare sector, the lack of good data security is a safety issue for individuals. For example, if a healthcare entity does not implement good data security and falls victim to a security incident or attack that results in either data accessibility or data integrity compromises (i.e., patient data is made either inaccessible or incorrect), the healthcare entity cannot treat patients, or may treat patients incorrectly, which could seriously affect the health or lives of the patients.

So, what does good data security hygiene look like from a cybersecurity perspective, particularly in the healthcare sector? How are healthcare entities supposed to keep up with a constantly changing risk landscape? What are the risks that the regulators are most concerned with and that healthcare entities should prioritize? These are all good questions; the answers are regularly discussed in Cyber Security Newsletters, a monthly publication by the Department of Health and Human Services (HHS), Office for Civil Rights (OCR), which is the primary regulator responsible for implementation and enforcement of the Health Insurance Portability and Accountability Act Privacy, Security, and Breach Notification Rules (HIPAA Rules).[2]

Although regulated entities are generally familiar with settlement agreements and civil money penalties (CMP) published by OCR,[3] and the insight they provide into the data security issues on which OCR is focusing its

enforcement efforts, many regulated entities are not leveraging the information contained in the Cybersecurity Newsletters[4] to augment their HIPAA Security Rule compliance efforts, particularly with regard to high-risk issues. Reviewing some of the most recent Cyber Security Newsletters is particularly instructive to understand recurring HIPAA Security Rule compliance issues that create cybersecurity risks for HIPAA covered entities and business associates.

HIPAA Risk Analysis: Identify ePHI and risks to it

The HIPAA Security Rule requires, as a foundational administrative safeguard for electronic protected health information (ePHI), that HIPAA covered entities and their business associates (as defined by the HIPAA Rules) undertake a comprehensive and enterprise-wide analysis (or assessment, as it is referred to in other economic sectors) of the risks, including threats and vulnerabilities to all of the ePHI they hold.[5] The requirement is essential for purposes of identifying all of an entity's data and the risks to it, including those associated with any cybersecurity threats or vulnerabilities that could be exploited by cybersecurity threat vectors or attackers.

This requirement is fairly straightforward; that is, HIPAA covered entities and their business associates must identify:

- the ePHI they hold, including through data inventories, mappings, and flows;
- the threats to and vulnerabilities of the ePHI, given the people, entities, and assets that create, access, maintain, and transmit such ePHI, including systems, applications, devices, workforce members, and partners; and
- the likelihood that these threats or vulnerabilities could be exploited, which is the risk to ePHI.

Essentially, this means that HIPAA covered entities and their business associates should understand where their ePHI is throughout its lifecycle (from creation to maintenance to destruction), and what the risks (including cybersecurity threats or vulnerabilities that could be exploited by cyberthreat vectors or attackers) to it are, given where it is created, accessed, maintained, and transmitted until it is destroyed.

The point is—if a HIPAA covered entity or business associate does not identify all the places where ePHI "lives," and the risks to ePHI in those places, then it cannot sufficiently protect the ePHI against threats or exploitation of vulnerabilities, which will very likely result in a breach.

However, HIPAA covered entities and their business associates often have misunderstood this requirement to be an audit or gap analysis, and instead of analyzing the risk to the ePHI, they assess the gaps in their enterprise practices against the requirements of the HIPAA Security Rule or another cybersecurity framework, such as the NIST Cyber Security Framework.[6] A gap analysis or audit is also a helpful exercise, and is required by the evaluation requirement of the HIPAA Security Rule at 45 CFR § 164.308(a)(8), but it is not a risk analysis.