SHUMAKER
Shumaker, Loop & Kendrick, LLP

Client Alert

Business Information for
Clients and Friends of
Shumaker, Loop & Kendrick, LLP

April 19, 2019

The Lack of an Adequate HIPAA Security Risk Assessment is a Common and Costly Mistake by Healthcare Providers: What Providers Can Do Now

Erin S. Aebel, Partner | eaebel@shumaker.com | 813.227.2357

Health care providers and others who must comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") have specific requirements under the Security Rule to HIPAA when it comes to their maintenance of electronically held protected health information. One of those requirements is to conduct a Security Risk Assessment and to update it periodically.[1] The HIPAA Security Rule defines a risk analysis as an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."[2]

In my practice as a board certified health lawyer representing health care providers of all sizes in business and compliance, I regularly see providers either fail to create a HIPAA Security Risk Assessment or they have one that the Office for Civil Rights ("OCR"), the government agency responsible for enforcing HIPAA, would deem inadequate. It is, in fact, one of the most frequently investigated HIPAA compliance issue by the OCR.[3] This can lead to monetary penalties and can also create risks that result in expensive security breaches that must be reported under HIPAA or state privacy laws such as the Florida Information and Protection Act of 2014 ("FIPA").[4]

For example, in 2018 Fresenius Medical Care North America was fined 3.5 million dollars by the OCR. The OCR found five separate breaches which were impermissible disclosures of electronic protected health information. In issuing the fine the OCR noted that the risk analysis was insufficient. Specifically, the OCR said "The number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprise-wide risk analysis for a covered entity."[5]

Health care providers should check now before they are dealing with a security breach or a complaint to the OCR, to confirm that they have an adequate HIPAA Security Risk Assessment in place. In its guidance in an April 2018 newsletter, the OCR lays out the elements that a risk analysis must include which are summarized below.

1. Scope of the analysis. The provider must review potential risks and vulnerabilities to the confidentiality, availability, and integrity of all the electronic protected health information ("ePHI") that an organization creates, receives, maintains, or transmits in any form and/or location.

2. Collect Data. The provider must identify where the ePHI is stored, received, and maintained by reviewing past and/or existing projects, performing interviews, reviewing documentation, and using other data gathering techniques.

3. Identify and document potential threats and vulnerabilities. The provider must identify and document reasonably anticipated threats to ePHI and vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of ePHI. These vulnerabilities could include holes, flaws, or weaknesses in information systems.

4. Assess current security measures. The provider must assess and document the security measures an organization uses to safeguard ePHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. Examples are encryption and anti-malware solutions, or the implementation of a patch management process.

5. Determine the likelihood and impact of threats. Next, the provider must consider the probability of potential risks to ePHI and document all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability, and integrity of ePHI. Then, the provider must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability and document all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability, and integrity of ePHI within provider's organization.

6. Determine the level of risk. The next step is for the provider to assess risk levels for all threat and vulnerability combinations identified during the risk analysis. The provider could document assigned risk levels and create a list of corrective actions to be performed to mitigate each risk level. Determining the levels of risks helps providers know their greatest risks so they can appropriately prioritize resources to reduce these risks.

7. Create documentation. Finally, the provider must document the analysis. The OCR does not require a specific format. However, since this is important proof that a provider conducted a risk analysis, the documentation should be detailed and easy for provider leadership to access, review, and provide to the OCR if necessary. According to the OCR, it should have sufficient detail to demonstrate that the provider's risk analysis was conducted in an accurate and thorough manner.

8. Periodic review and updates to the risk analysis. Importantly, the provider must conduct a continuous risk analysis to identify when updates are needed. The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. One idea is to set a date to review the risk analysis at least annually or more frequently if there has been a security breach of ePHI.[6]

The OCR goes on to explain that a gap analysis is not a sufficient risk analysis for a provider. A gap analysis is typically a high level review of what controls are in place (or missing) from a provider's compliance with particular aspects of the HIPAA Security Rule. While a gap analysis may be helpful to a provider's overall HIPAA Security Rule compliance, it does not assess the risks to all the ePHI a provider creates, receives, maintains, or transmits. Therefore, it fails to meet the standards for a required security risk assessment.[7]

A provider may work with an inside or outside IT professional and a health care lawyer to make sure the security risk assessment is adequate. However, some vendors may claim they are "HIPAA compliant" without fully understanding the specific HIPAA risk assessment requirements the OCR is looking for. Accordingly, the provider and their counsel need to review the risk assessment to make sure it is a thorough review hitting all of the above points. Getting this done now when there is not a breach or complaint may save the health provider a lot of time and money in the future.

If you have any questions, please contact Erin S. Aebel at eaebel@shumaker.com or 813.227.2357 .

---

[1] 45 C.F.R. § 164.308(a) (1)(ii)(A).

[2] Id.

[3] See, Enforcement Results of February 28, 2019, https://www.hhs.gov/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[4] See, Fla. Stat. § 501.171.

[5] See, HHS Press Release, Five Breaches Add Up to Millions in Settlement Costs for Entity that Failed to Heed HIPAA's Risk Analysis and Risk Management Rules, February 1, 2018.

[6] See, OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule, Posted by the OCR July 14, 2010.

[7] See, OCR Newsletter, Risks Analysis vs. Gap Analysis – What is the Difference? April 2018.