Health Information Compliance Alert

Toolkit: Don't Shirk on Analyzing Your Risks in Times of Crisis

Tip: Use your firm's data to configure a risk management plan.

You may think that with some parts of HIPAA relaxed during the COVID-19 pandemic that you don't need to worry about privacy and security. But for the majority of circumstances, the HIPAA Rules still apply and that means you should continue to be vigilant, especially with the transfer of your electronic data.

Context: With so many healthcare operations going digital during this public health emergency (PHE), it is critical to keep on top of your compliance concerns. Remember that risk analysis "is one of four required implementation specifications” in the HIPAA Security Rule, reminds **HHS Office for Civil Rights** (OCR) guidance. Covered entities (CEs) are required to "conduct 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 [organization],” OCR cautions.

Heed This Expert Security Rule Insight

You can stave off violations and crippling fines by performing a thorough HIPAA risk analysis in order to comply with the Security Rule, if you haven't already. The first step in the risk analysis is to look at the "big picture” to identify potential risk points, says HIPAA expert **Jim Sheldon-Dean,** founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont.

Start by identifying what systems are holding onto electronic health information that contains PHI, including electronic health records (EHRs) and business files, Sheldon-Dean advises. "Look at how those systems move information within the entity, as well as to business associates outside the entity or to other entities for other purposes.”

After identifying the risk points, do a more detailed risk assessment of your individual systems. You identify their specific risk points, as well as significance - and the likelihood that a problem will occur, and then address it, Sheldon-Dean instructs.

There are several ways to do the risk analysis assessment, he adds, but the simplest approach is to use a methodology defined by the **National Institute of Standards and Technology** (NIST) special publication on risk analysis.

Add These 8 Steps to Your Security Planning

Since the HIPAA Security Rule requires you to assess your organization's risks and put them into a written risk analysis, you'd think there would be a format - there isn't. But that gives your compliance team some leeway to design a system that accurately measures and manages your risks.

Consider adding the following steps from the **Centers for Medicare & Medicaid Services** (CMS) and OCR into a personalized template and develop your own process.

1. Identify the scope: Your risk analysis should encompass all the potential risks and vulnerabilities to all the protected health information (PHI) that your practice creates, receives, maintains, or transmits. This includes all PHI and electronic PHI (ePHI) in all forms of media, which can include paper documents, CDs, hard drives, mobile devices, transmission media, electronic storage media, and much more.

2. Gather data: Begin compiling data on where you store, receive, maintain, or transmit PHI. You may need to look at

CPT® 2023 American Medical Association. All rights reserved.

more than a single department - check out any data exchanges between vendors and business associates, as well as any PHI in different physical locations or electronic media. Also, you must document how, when, and what data-gathering activities you performed.

3. Pinpoint potential threats and vulnerabilities: You're not looking for any and all conceivable threats, but instead you should identify and document all "reasonably anticipated” threats. Examine threats based on these categories:

- Natural - Floods, earthquakes, tornadoes, landslides
- Human - Intentional or unintentional actions (e.g., unauthorized access to ePHI network and computer-based attacks, malicious software upload, inadvertent data entry or detection, inaccurate data entry)
- Environmental - Power failures, pollution, chemicals, liquid leakage

4. Assess current security measures: Compare your existing security measures with the potential threats and vulnerabilities you've identified. Evaluate all your security measures (technical and non-technical), such as your access controls, authentication, encryption methods, automatic logoff, and audit controls, as well as your policies, procedures, guidelines, accountability, and responsibility, and physical and environmental security measures.

5. Ascertain the likelihood of threat occurrence: Weigh the probability that a threat will trigger or exploit a particular vulnerability, and then estimate the potential impact on your organization. Categorize each specific threat as "high likelihood,” "medium likelihood,” or "low likelihood.” Use your determinations to create a list prioritizing your risk mitigation efforts.

6. Determine the potential impact of threat occurrence: Estimate the possible threat's potential outcome or impact. This may include unauthorized access to or disclosure of ePHI; permanent loss or corruption of ePHI; temporary loss or unavailability of ePHI; loss of physical assets; or loss of cash flow. Similar to ranking likelihood, organize the potential impacts as "low,” "medium,” and "high.”

7. Deduce the level of risk: Cross-reference the likelihood rankings with the potential impacts to determine your risk level for each identified threat. Risk ranking helps you to prioritize mitigation activities - meaning, what you should fix first. Look at any potential threats that rank "high” on both the likelihood and impact scales.

8. Identify security measures and finalize documentation: Beginning with the highest-risk items, identify the security measures necessary to manage the risk. When evaluating appropriate security measures, consider their:

- Effectiveness;
- Related legislative or regulatory requirements for implementation; and
- Relation to your own organization's policies and procedures.

Small practice advice: You can create a risk analysis report to document your process, the output of each step and your initial identification of security measures, the feds suggest. "The risk analysis needs to clearly relate to your own practice, and a small practice with limited use of electronic PHI would look much simpler relative to a large multisite medical group,” said **Glenn D. Littenberg, MD, MACP, FASGE, AGAF,** a gastroenterologist and former CPT® Editorial Panel member in Pasadena, California.

"Much of this burden shifts to entities that host data on their clouds, but the practice still has to look at how it uses PHI in any electronic form and that there are security rules and processes, such as what to do in case of breach,” Littenberg said.

Resources: Find the NIST guidance at https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final and check out the OCR's HIPAA Security Rule summary at www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

CPT® 2023 American Medical Association. All rights reserved.