Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: Assess Your Risks Now to Avoid Problems Later

Tip: Use security measures that fit the scope of your practice.

It should come as no surprise that as data incidents have multiplied, the HHS Office for Civil Rights (OCR) has stepped up its HIPAA enforcement. With million dollar settlements becoming more prevalent, it's critical that you meet the risk analysis demands outlined in the HIPAA Security Rule. Because, if you find yourself on the wrong side of a breach, the first thing the feds will ask for is how you've managed your risks.

Privacy Rule Isn't the Problem

Practitioners and administrative staff find it much easier to wrap their heads around the HIPAA Privacy Rule, suggests **Adam Kehler, CISSP**, principal consultant and healthcare practice lead with **Online Business Systems**. The rise of health IT, however, puts the security of electronic protected health information (ePHI) at the forefront of compliance and securing that data is much more complicated.

"Consider an analogy to cooking: Suppose a recipe says 'Add as much milk to your recipe as is reasonable and appropriate.' This may make sense for someone who is an experienced chef, but to the person at home just trying to follow a recipe, they have no idea how to determine 'reasonable and appropriate.'” Kehler explains. "It's the same thing with calculating risk.”

He continues, "The HIPAA Security Rule requires that organizations implement 'reasonable and appropriate' security controls based on their assessment of risk. Most professionals who studied medicine or health administration are not in a position to make these decisions.”

Add These Requirements to Your Risk Analysis

Not only is assessing your practice risks smart business, but it's an administrative safeguard provision under the HIPAA Security Rule. "The Security Management Process standard in the Security Rule requires organizations to 'implement policies and procedures to prevent, detect, contain, and correct security violations (45 C.F.R. § 164.308(a)(1)'” OCR guidance reminds.

Definition: "Risk can be understood as a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization,” notes the **National Institute of Standards and Technology** (NIST) Guide for Conducting Risk Assessments. "This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.”

Consider these basics as you pinpoint your practice's HIPAA shortcomings:

- Discern what constitutes ePHI in your practice. Hint: "This includes ePHI that you create, receive, maintain or transmit,” says NIST.
- Identify your business associates, vendors, suppliers, and partners that handle your patients' ePHI and manage those risks with agreements and compliance.
- Recognize the IT threats and outline them in your analysis.
- Implement your plan based on your findings to address vulnerabilities.
- Follow up often on your compliance protocols and manage the threats to ePHI with network logging, audits, pentests, patch management, and more.
- Encrypt your mobile devices and use multi-factor authentication on passwords.

- Think ahead and write up an incident response plan.

Tip: "By assessing the risk to the organization based on system criticality, threat levels, and business impact, organizations can prioritize their security spending for the greatest benefit," advises Kehler.

Resource: See more federal guidance on assessing risk at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.