Codify
BY AAPC

MDS Alert

Policies and Protocols: Conduct Regular HIPAA Security Rule Risk Analyses

The OCR is stepping up its enforcement.

With cybercriminals becoming smarter, long-term care industry staff turnover rates as high as ever, and Health Information Portability and Accountability Act (HIPAA) breaches increasing, your facility needs to be shipshape in its barriers against protected health information (PHI) breaches. The HHS Office for Civil Rights (OCR) has stepped up its HIPAA enforcement, and million-dollar settlements occurrences are increasingly frequent. Make sure you have the requisite policies and protocols in place, so if a breach investigation occurs, you can show that you've done your homework on managing your risks.

Security Rule Growing in Significance

Clinical leadership 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 information technology (IT), however, puts the security of electronic protected health information (ePHI) at the forefront of compliance, and now securing that data is much more complicated.

"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," Kehler says.

"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,'" he explains. "It's the same thing with calculating risk."

Hit These Hot Spots in Your Risk Analysis

Not only is assessing your facility's risks smart business, 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 says.

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 facility or organization's HIPAA shortcomings:

- Discern what constitutes ePHI in your facility. Hint: "This includes ePHI that you create, receive, maintain or transmit," NIST says.
- 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, including laptops, 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.

Implement Continuing Education

The long-term care industry faces notoriously high staff turnover. Make your facility's HIPAA policies and protocols a standard part of your facility's onboarding for new employees. Integrate basic information about HIPAA into your training, as well as specific risks and example scenarios. Consider bringing in a professional consultant to conduct the HIPAA training, as an expert will know the ins and outs of both the Privacy Rule and the Security Rule and can deftly answer any questions.

Don't forget your current employees: Make HIPAA training part of continual education as well, with refresher courses annually, and make sure all employees who use a computer or have access to EHR - across all departments - attend. If your facility has an IT department, make sure team members are at the HIPAA trainings so they have a working knowledge of what exactly constitutes an electronic breach. Do your best to cultivate an open culture between those employees and everyone else, so all staff feel comfortable going to IT if they are worried about having clicked on what might be a phishing email or any other potential ePHI breach scenario.

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