Health Information Compliance Alert

Risk Analysis: Assess Where Your Practice is the Most Vulnerable

Hint: Staff education should be at the top of your to-do list.

According to the HHS-OCR breach portal, 2017 is turning out to be a banner year with 84 breaches reported so far, impacting over 1,730,000 people since Jan. 1. With odds like these for just the first quarter alone, it's time to accept that HIPAA breaches big and small happen no matter how thorough the compliance plan.Visit the HHS-OCR breach portal at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Review time: Doing an internal risk assessment is a good place to start and will help you determine where your practice is the most vulnerable. Take a look at these five areas where compliance expert **Brand Barney, CISSP, HCISPP, QSA,** a security analyst with Security Metrics in Orem, UT sees practices losing ground in the healthcare compliance and security game:

1. Human Error: Most violations are caused by staff accidentally due to a lack of education on HIPAA security. "Fix your people. They are prone to human error," Barney recommends. "You can buy a super cool product [CEHRT], but unfortunately your people don't know how to use it." And that's a problem.

2. Configurations: Once you get past the privacy part, security is about properly configuring your system. "The tools aren't necessarily plug-in and play. A lot of these devices come with defaults to allow access to networks, but proper configuration of them is massively important," Barney advises. "It can be as simple as a well-configured firewall that stops attackers from accessing your PHI."

3. Logging and Monitoring: This area of the HIPAA security rule is critical and often overlooked or not properly followed. "Practices should be looking at the integrity of the systems; oftentimes they don't," Barney says. And if you don't, "How do you know when there's a problem?"

For example: "They [systems] continue to blast with alerts but the staff has no training. They find it too noisy and turn it off. So when there's a real breach they have no idea," Barney cautions. "If you have no logging and monitoring mechanisms, you are in deeper than you want to be." He adds, "I can't stress this piece enough. Properly log and monitor your networks and systems. Attackers are banking on you having no insight, then they walk away with your data, and you are none the wiser."

4. Business: You should consider all vendors and business associates that can impact the PHI/ePHI environment," Barney says. "It is easy to identify that you share data with a billing service provider, but are you identifying that HVAC vendor that has remote access to your networks?"

Planning a business associate agreement is more than just the paperwork all parties that create, receive, transmit, and maintain your practice PHI and/or ePHI must be included, he adds. "Once you have identified them you should consider processes for them to demonstrate that they are truly handling your security and their own in a satisfactory method."

5. Policies and Procedures: After you've assessed, analyzed, and implemented security to comply with HIPAA, you must prove it in writing. "Documentation is key," Barney says. And before they investigate your breach "the OCR will say, 'Shoot us your policies and procedures.' And they are going to go in with the assumption that you've done nothing, especially if you have no documentation."

Moreover, "privacy is usually documented quite well by most practices. But when it comes to detailing policies and procedures for the HIPAA Security Rule items like incident response plan, encryption, firewall configuration standards, emergency mode operations entities are negligent," he points out.

Remember: Steep penalties may ensue if you don't have your ducks in a row. "Through recent settlements, the OCR has demonstrated its propensity to impose significant fines on entities that fail to implement appropriate safeguards, independent of the number of affected individuals or the content of the protected health information included in a particular breach," reminds attorney **John E. Morrone, Esq**, a partner at Frier Levitt Attorneys at Law in Pine Brook, NJ.