Codify
BY AAPC

Health Information Compliance Alert

Case Study: Compliance is Just One Piece of the Security Puzzle

Hackers only need one point of entry to wreak havoc on your health IT.

A top-notch HIPAA compliance plan won't get you brownie points with the HHS Office for Civil Rights (OCR) anymore. It is expected and must be outlined should a breach occur. And just because you have it doesn't mean your practice systems are secure.

Background: ABCD Pediatrics in San Antonio, TX discovered a cyber attack in February due to ransomware that was impacting its encrypted data. Luckily, the digital takeover was slowed due to antivirus software, and the practice swiftly alerted their IT company about the issue. "ABCD's IT Company identified the virus as 'Dharma Ransomware,' which is a variant of an older ransomware virus called 'CriSiS,' the practice news release said. Read the ABCD Pediatrics release at: http://www.abcdpediatrics.com/HIPAANotificaiton/.

Impact: Analysis of the offline servers showed "hackers may have accessed portions of ABCD's network," impacting 55,447 individuals, the HHS-OCR breach report suggests. However, the IT firm "found no evidence that confidential information was actually acquired or removed from its servers and computers," ABCD's release stated. But "it could not rule out the possibility that confidential information may have been viewed and possibly was acquired."

Consider this: ABCD had a comprehensive cybersecurity and HIPAA plan that included "network filtering and security monitoring, intrusion detection systems, firewalls, antivirus software, and password protection." But many practices don't, and their breaches are far worse than ABCD's and electronic protected health information (ePHI) is not only lost but utilized by the cyber criminal.

So why aren't healthcare organizations more prepared for this kind of crime? "The number one issue is lack of awareness that this can happen," says **Kurt J. Long,** founder and CEO of FairWarning, Inc in Clearwater, Fla."Providers are worried about patients and focused on patient care and for whatever reason many practices of all sizes are remarkably unaware of the threats."

Move Beyond Privacy Protection and Invest in Security

So what happens to the provider who protects patient privacy by following the HIPAA Privacy Rule to the letter but doesn't take into account the Security Rule?

"Oftentimes these providers are doing a good job with the Privacy Rule," notes **Brand Barney, CISSP, HCISPP, QSA,** security analyst with Security Metrics in Orem, UT. "And they think they're compliant and in 100 percent of the cases I've seen that is not what I uncover."

What happens is they invest in advertised HIPAA-compliant solutions that they've seen at a conference, in an email plug, or on a webinar and assume they are now in compliance, Barney suggests. "But 9 times out of 10 that is patently false. Those tools are fantastic but are dependent on you [the staff] using them properly," he points out.

Cyber know-how: If you've got a handle on protecting PHI in the office, your next move should be a risk analysis by a compliance expert because it is a lot for one person or even a large in-house IT team to take in without skilled input. "[Health IT security] is overwhelming for someone whose every day is devoted to this," Long reminds. "The level and sophistication [of hackers] has grown so dramatically in years that even a moderately practiced health IT team can't handle the issues."

Next steps: "There are many pieces to security, and it can be expensive," Barney says. "And it can be an uphill battle to get stakeholders to support it." Practices need to look beyond the firewalls, network monitoring, and programs, he

reasons. "Security is tough, and it's mission critical. It should not be convenient."

Compliance and security need to go hand-in-hand because people's lives are at stake when a system is compromised. Before you reach out to a compliance specialist, consider doing these three things to help with a risk analysis:

- Make sure your HIPAA policies and procedures are up-to-date and meet the latest privacy and security requirements;
- Create a list of all business associates (BAs) that provide services to your organization; and
- Conduct an internal risk assessment to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Tip: "Put this piece of the pie [security] back in with the full healthcare experience," says Barney. "The same mentality that you have for helping the patient ensuring their long-term care and privacy, should be used to protect their data, and the confidentiality and integrity of it and yours."