Health Information Compliance Alert

Cybersecurity Quiz: Test Your HIPAA Security Prowess

Tip: 2018 is ramping up to be a banner breach year - prepare now.

The HHS Office for Civil Rights (OCR) 2018 wall of shame is currently at 70 reported breaches and counting, and it's only April. The long and varied portal, which only focuses on large-scale cases of 500 or more affected individuals, suggests that providers big and small can never be too careful when securing patients' protected health information (PHI) and ePHI.

Among the plethora of HIPAA violations, most concern lost ePHI and fall under the umbrella of cybersecurity. Experts caution that lackluster safety protocols and failure to identify risks can lead to major losses - both financial and professional - that add up quickly.

Reminder: "Healthcare has traditionally been less sophisticated when it comes to information security ... [but] now is the time to get serious about protecting systems, because lives and institutions are at stake," warns HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont.

Familiarizing yourself with cyber thugs' modus operandi will help you safeguard against attacks and thefts, saving you time, money, and headache. Test your cybersense with the following five questions based on information from past issues of Health Information Compliance Alert.

Question 1: Everyone in your practice is crazy about this new cardiology blog that offers tips and advice for specialists in the field. Clinical staff frequent the site often throughout the workday from their various devices throughout the office. But, after months of utilizing the online resource, staff computers start to lag and employees have problems downloading information. One Monday morning the entire group is locked out of the system. What might have happened?

Answer: What may have transpired involves two different, but similar, forms of phishing techniques aimed at preying on providers' habits. Specialists, who naturally look up medical information repeatedly on the same site, may end up being targeted by "pharmers" while a group of specialists researching a particular topic are usurped by the "watering hole" tactic.

Both harness common interests and log how often a site is visited. Hackers use the information to either direct you to an identical but false page, stealing your passwords and controls, or install malware to the popular link and infiltrate your office system with it. Once inside your network, cyber criminals can wreak all sorts of havoc, including the hijack of patients' ePHI.

Question 2: Every day when you log into your laptop, a little reminder pops up asking you to install the latest Microsoft patch for the software your hospital utilizes. Your IT manager says just click "remind me tomorrow," but tomorrow turns into weeks. Before you know it, the entire hospital network is down. What could have stopped the outage?

Answer: Software patch management and stricter security protocols would have closed up the loophole that let hackers in. Technology coordination between vendors and HIT staff ensure compliance. From Petya to WannaCry to Spectre to Meltdown, healthcare has been ravaged by the lack of patch maintenance over the last 12 months.

"Cyber criminals prey upon lax security practices; most breaches and attacks are preventable through a higher prioritization of operational security, including patch management and aggressive training programs," observes **Kurt J. Long**, founder and CEO of FairWarning, Inc in Clearwater, Florida. "Apply vendor recommendation patches aggressively, and watch for vendor updates vigilantly."

Tip: Long advises, "Not only should your IT team remain on top of such updates, but also, they should be driving a security-centric culture through your organization."

Question 3: You just moved from a small-town clinic to a large, urban group practice. The IT person okayed the use of your personal devices under the practice's Bring Your Own Device (BYOD) policies, but he insisted that software to monitor practice data be installed for security reasons. Why?

Answer: Smartphones, laptops, and tablets allow physicians to assist patients anywhere and at anytime. However, despite this convenience, lost and stolen devices accounted for a significant number of breach cases over the last few years, exposing millions of patients' ePHI.

Large-scale medical systems now utilize Mobile Device Management (MDM) software and governance to protect assets and patients. Certified EHR Technology (CEHRT) vendors offer additional coverage of mobile devices with applications to help providers combat this common issue, too. The OCR and the Office of the National Coordinator for Health Information Technology (ONC) also provide advice and insight on how to implement compliant MDM programs. (See p. 28)

Question 4: You move your pediatric practice into a new facility in a different state with new partners and staff. When you shutter your old business, your previous practice manager throws the old software, hardware, andpaper files into the dumpster since you won't need the materials or the data anymore. What's wrong with this scenario?

Answer: Everything! The OCR has specific instructions for how PHI and ePHI is disposed of whether a practice is open or closed. In fact, the agency advises covered entities to strictly follow risk management protocols when dealing with information after a business goes under. Some of its suggestions include:

- Shred, burn, pulp, or pulverize records that contain PHI, ensuring that the information is thoroughly indecipherable and destroyed.
- Clear, destroy, wipe, overwrite, purge, and destroy any electronic media that contains ePHI.

See the OCR's PHI and ePHI disposal advice at: www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html?language=en.

Warning: "Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI," reminds the OCR guidance. "Further, covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member."

Question 5: Mrs. Smith abruptly departs your practice after 20 years as a nurse practitioner. During a routine systems check, your IT manager notices remote log-in access and irregularities. What may have occurred?

Answer: It's likely in this example that Mrs. Smith illegally accessed the network for nefarious reasons for things as varied as stealing practice secrets to the theft of patients' ePHI. Small practices are often too trusting while big healthcare groups may be too busy to notice the comings and goings of employees. But, it can be hard to justify these types of excuses with so many resources out there to help avoid HIPAA pitfalls.

"I think being busy or the 'that won't ever happen to me' logic may come into play," says attorney **Kathleen D. Kenney** of Polsinelli LLP in Chicago. "Ultimately, I think this issue, like many HIPAA issues that arise, stems from a failure to implement processes and ensure checks and balances are in place when it comes to security."

Tip: Logging and monitoring your systems are two of the most crucial actions in managing cyber risks, according to compliance expert **Brand Barney, CISSP, HCISPP, QSA**, a security analyst with Security Metrics in Orem, Utah. This area of the HIPAA security rule is critical and often overlooked or not properly followed, he warns.

"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?"