Health Information Compliance Alert

Toolkit: Update Your Digital Dictionary With These Additions

Keep your security game in top form with new cyber slang.

Safeguarding patients' electronic protected health information (ePHI) is vitally important and is required under the HIPAA Security Rule. But evidence suggests that healthcare remains a hot spot for hackers with IT incidents on the rise. It's critical that you keep abreast of the everchanging cybersecurity conversation to keep threats at bay.

Background: According to the feds, practices must have their guards up to combat hackers. "We are under constant cyberattack in the health sector, and no organization can escape that reality," warns **Eric Hargan,** HHS deputy secretary in the agency's release, Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients. "While innovation in health information technology is a cause for optimism and increasing sophistication in health IT holds the promise to help address some of our most intractable problems, whether in clinical care, fundamental research, population health or health system design, our technology will work for us only if it is secure."

Check Out These 8 Cyber Must-Knows

That's why staying on top of the latest terms and techniques is essential to avert the risks. Consider plugging these hot topics into your cybersecurity playbook for future reference:

1. Advanced Persistent Threat: "An advanced persistent threat (APT) is a long-term cybersecurity attack that continuously attempts to find and exploit vulnerabilities in a target's information systems to steal information or disrupt the target's operations," according to the **HHS Office for Civil Rights** (OCR) spring 2019 issue of the Cybersecurity Newsletter. APTs aren't always sophisticated cyber attacks, but the hackers' ability to sidestep detection make them lethal to healthcare, the OCR reminds.

2. Drive-by Download: Protecting personal data is critical in medicine, and drive-by downloads are so subtle that cyber thugs infiltrate systems before users even know what's happened. When users unintentionally download malware to their computers, it's considered a drive-by download. "What sets this type of attack apart from others is that users need not click on anything to initiate the download," says IT security company, **Trend Micro,** in online guidance. "Simply accessing or browsing a website can activate the download."

3. EHR Vendor Lock-in: A great reason to do a background check on your EHR vendor is to look into proprietary tactics that a vendor might use to thwart you from using other products. When you can't access other EHR vendors' products without paying an exorbitant cost to get out of your current situation, that is an EHR vendor lock-in. Review your EHR and cloud-provider contracts before implementation to avoid this problem later on.

4. Honeypot: In a nutshell, a honeypot is a decoy server that draws hackers to it, similarly to the way honey attracts bears. Because IT staff can see cyber thugs homing in on this target in the network, they can use the honeypot as a tool to fix practice issues.

5. Identity Assurance: As the feds push to put more power in the hands of patients, providers must consider identity management a part of their daily information gathering before they deliver care. Identity assurance is a two-pronged system that includes vetting and confidence in credentials, according to the **HHS Office of the National Coordinator for Health Information Technology** (ONC). And by way of identification checks, both physical and electronic, identity "assurance answers the question, 'How sure am I that you are who you say you are?'" explains ONC.

6. Metadata: Sets of data that explain information and detail its use are called metadata. Within metadata there are three subcategories: administrative, descriptive, and structured. "Metadata [is] structured information that describes, explains, locates, and otherwise makes it easier to retrieve and use an information resource," explains an **American Health Information Management Association** (AHIMA) brief on the subject. For example, when the details of a document are given - creator, date, and file size - to explain the information, that is metadata.

7. Pentest: Professionally known as a penetration test, a pentest is a simulated cyber attack that is usually carried out by IT staff to check for security risks in a system. If your practice IT is handled by an outside resource, you'll need to request pentest reports to ensure that your ePHI is being stored and transmitted securely, advises **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. "Pentest reports are a good way to ensure they protect your patients' information."

8. Zero-Day Vulnerability: When your system is ripe for a cyber attack but you're unaware of any problems, that is a zero-day vulnerability. "Hackers may discover zero-day exploits by their own research or probing or may take advantage of the lag between when an exploit is discovered and when a relevant patch or anti-virus update is made available to the public," the OCR Cybersecurity Newsletter says.

Tip: Risk planning must include assessment, analysis, and management to ensure HIPAA Security Rule alignment and minimize the chance of a cyber attack. From device management to staff training to contingency planning, your compliance protocols should outline how you're going to stop malicious attacks and what you'll do if one occurs at your practice.

Resource: For a closer look at the spring 2019 edition of the OCR's Cybersecurity Newsletter, visit www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-spring-2019/index.html#footnote1_es3lguw.