Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity Quiz: Test Your Cybersecurity Smarts With These 10 Questions

Tip: Make staff training a priority in 2020.

Data security continues to be the Achilles heel of healthcare. From the gambit of social engineering incidents to encryption snafus, the industry suffered mightily in 2019 with major setbacks that impacted millions of patients' electronic protected health information (ePHI).

Manage Risks With Analysis and Training

Once you dig into the details of many healthcare-related cyber attacks, two things often pop out: - a lack of risk management policies and protocols and limited or no staff training on cybersecurity. That's why it's critically important that management promote compliance by advocating for better employee education on data security as well as stronger risk planning, explains HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont.

"You have to start at the top," stresses Sheldon-Dean. "There needs to be a corporate commitment to privacy and security, and the first step is to establish the responsibility and authority to make sure the organization as a whole, as well as all elements of the organization, make the plans and have the necessary resources ready to conduct risk analyses, from the corporate to the local office level."

Sheldon-Dean adds "This requires that there are overarching policies and procedures for privacy and security providing the authority within which the work can be performed."

Reminder: Hackers aren't particularly picky either; moreover, recent incidents highlight more than ever that organizations of every size and scope remain vulnerable to attack. "A lot of my customers think they're too small to be targets, and maybe that's true, but the non-targeted attacks are still out there," warns **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah.

Tip: A great way to stay on track in 2020 is to review cybersecurity basics as well as emerging threats. Test your cybersense with these 10 tough questions.

1. What kind of software helps to prevent a ransomware attack?

a. Certified electronic health record technology
b. Cloud solutions
c. Anti-virus software
d. Slack messaging

2. What decoy tool can you use to distract and draw hackers?

a. Honeypot
b. TrickBot
c. Encryption
d. Vishing

3. What is a nickname for a cyber attack simulation, usually performed by IT staff?

a. RiskIT
b. Pentest
c. APT
d. API

4. What social engineering tactic uses malware to lure victims via SMS texting to reveal personal or practice information?

a. Pharming
b. Smishing
c. Vishing
d. Firewall

5. What is patch management?

a. The application of vendors' security updates in a timely manner
b. A badge protocol at the hospital
c. How Medicaid monitors health IT
d. None of the above

6. What important action are you taking when you encode data, so that only authorized users can see and use it?

a. Patient blocking
b. Risk assessment
c. Software update
d. Encryption

7. What are you implementing when your systems prompt you to report at least two types of evidence to authenticate your identity during the log-in process on your devices?

a. Password safe
b. Breach list
c. Multi-factor authentication
d. Techguard

8. What can you install to block out unauthorized users while also monitoring network traffic?

a. Malware
b. Spyware
c. Application Programming Interface
d. Firewall

9. What is it when your practice is exposed for a cyber attack, but you don't know it?

a. Man-in-the-middle
b. Zero-day vulnerability
c. Open source
d. Cloud opening

10. What hack are cyber criminals utilizing when they use legitimate-looking software, trick you to download, and then destroy your device via the back door?

a. Tailgating
b. Spearfishing
c. Trojan horse

d. Worm

Answers: 1) c 2) a 3) b 4) b 5) a 6) d 7) c 8) d 9) b 10) c