Health Information Compliance Alert

Cybersecurity Quiz Answers: Bolster Your HIT Security With These Facts

Tip: Close the door on hackers with better patch management in 2022.

Check your cybersecurity smarts against these answers.

Answer 1: A password manager is a software application that works as a virtual vault, housing your passwords on your computer, keeping them safe, and securing them with encryption. Password controls are particularly important in the healthcare setting, with not only critical patient data to protect but also the private information of your employees and organization.

A password management tool is an excellent resource to assist with password storage, says **Jen Stone**, MCIS, CISSP, CISA, QSA, principal security analyst with Security Metrics in Orem, Utah. "In my experience, the best passwords come from a password manager. They can be long, complex, and unique without taxing your ability to remember all the passwords to all your accounts," she adds.

But, remember the password management software must work with your current systems. "Use a password safe that is compatible with all of your devices," cautions **Adam Kehler**, Director of RSP Healthcare Services at Online Business Systems.

Answer 2: False. Vulnerability scans are automated programs that assess your network, searching for chinks in your IT armor - and they can be extremely helpful tools for analyzing your HIPAA security. "As part of the risk analysis, use [the] results of automated tools, such as network-layer vulnerability scans and application-layer code security scans, to give you a reality check on the state of the systems in your ePHI environment," Stone advises.

On the converse, a penetration test or pentest for short is a professionally-simulated cyber attack on your network that is performed by IT security experts. The information garnered from the pentest will help your organization figure out where your systems need to be fortified. Plus, they offer IT staff an additional HIPAA Security Rule-related bonus, Stone says. "Pentest reports are a good way to ensure they [are] protect[ing] your patients' information."

Answer 3: True. Hashing is "the process of using a mathematical algorithm against data to produce a numeric value that is representative of that data," according to the National Institute of Standards and Technology's (NIST) Computer Security Resource Center definition.

Encryption also reworks data, but it uses cryptographic methods to turn the information into ciphertext. Another difference: Once data is hashed, it cannot be changed back to its original state; however, encrypted data can be decrypted.

Answer 4: C) improves the way your hardware looks. Patch management deals with software updates, but does not impact the visual appeal of your hardware. Keeping on top of software updates on your devices does, however, help the hardware work better by improving the software's efficiency, figuring out vulnerabilities in the system, and fixing bugs.

Answer 5: Machine learning is a type of artificial intelligence (AI) that uses algorithms to help clinicians predict illnesses and patient health risks, organize treatments, and improve healthcare outcomes.

Answer 6: False. If your practice falls victim to a ransomware or other malware attack, your first impulse is likely going to be to turn everything off. Depending on the type of data breach, you may want to keep systems running and consult a cybersecurity expert ASAP.

"When an organization finds out they have an incident such as ransomware, the temptation is to immediately power down the systems and wipe drives. In doing so, they may actually be destroying evidence that could be useful in investigating the incident," Kehler says.

Answer 7: D) all of the above. Keylogger software records the keystrokes that a device user hits, and then puts that logged information to nefarious means. Hackers use these points of access - email attachments, pop-ups, or infected websites - and more to infiltrate your systems by adding keylogger software. The primary problem is that the malware is usually added without the user even knowing. But, once the hackers have access to your system, they can cause all sorts of trouble for you and your organization.

Click here to go back to the quiz.