Health Information Compliance Alert

Quiz: See If You Are Up-To-Date on HIPAA Compliance

Hint: An EHR contingency plan is a safer bet than a generator in a natural disaster.

HIPAA compliance is something that should be part of your daily operations and is now essential to the success of your practice. Ignoring both the privacy and security requirements could open you up to dozens of violations.

Test your knowledge of HIPAA and compliance with the following ten questions based on information from past issues of Health Information Compliance Alert.

1. You head a very busy pediatric office, and your staff regularly use sign-in sheets to ensure they don't forget a patient in the queue. To avoid a violation, they can:

A. Limit information to name only on the sign-in sheet
B. Call out the patient by the name listed on the sign-in sheet only
C. Refrain from any mention of the reason for the visit
D. All of the above

2. Your practice decides to get rid of your outdated office hardware for new laptops. What do you do with the old computers?

A. Throw them out back in the dumpster.
B. Store them in the office storage room for back-up.
C. Extract the hard drives, strip and destroy the data, and dispose of the computers.
D. Give them to the IT officer for his home office.

3. Mobile devices and laptops, particularly ones that physicians and staff use in the office and remotely to access ePHI, should always include:

A. Encryption and multi-factor authentication that is updated frequently and outlined in an office HIPAAplan.
B. A case to protect the device from breakage.
C. Quick-and-easy passwords the whole office knows to increase workflow.
D. Software that makes it easier to get to EHRs.

4. Business is booming, so you've decided to outsource your billing to ABC Billing, Inc.. Before you send them your claims, you should:

A. Check the vendor's background and how they've complied with HIPAA in the past.
B. Ask for recommendations from other medical practices and follow up.
C. Institute a business associate agreement drawn up and organized by a lawyer who specializes in healthcare law.
D. All of the above.

5. Your new receptionist answers a call from an angry radiologist, insisting that she fax the files of five of your patients to his office immediately. When she asks the physician for his credentials, he screams at her outraged and hangs up. There is no follow-up call nor email from a radiology firm, which makes the call suspect and suggests:

A. The radiologist will file a complaint against the receptionist.
B. The caller was a social engineer scamming the practice for PHI.
C. It was a wrong number.

D. None of the above.

6. A power outage due to a vicious thunderstorm knocks out the electricity and your CEHRT. Luckily, you are prepared with a HIPAA-secure contingency plan. Your protocol includes:

A. Shelter for your patients.
B. A generator to bring the power back up.
C. An operations plan that allows your practice to run smoothly in the face of an EHR shut-down.
D. Food and water.

7. Your IT monitoring systems annoy everyone in the office so, you turn them off. When your IT director gets back from maternity leave, she reads through the reports and uncovers a breach. How could the violation have been prevented?

A. Staff education on the HIPAA Privacy Rule.
B. A business associate's agreement.
C. Logging and monitoring the integrity of the systems and networks daily for unusual activity.
D. A risk assessment.

8. Your practice manager opens an email from an affiliated hospital on Monday. On Tuesday, he comes in and is locked out of the system. What should he do?

A. Log-in with another co-worker's password and see if that works.
B. Alert the IT officer immediately that there's a problem in case of a cyber attack.
C. Use another computer until the glitch goes away.
D. Shut down the computer and go to lunch early.

9. Your IT security uncovers that a former employee has been accessing and stealing patients' data remotely. How did this likely happen?

A. The networks weren't configured right.
B. The compliance plan lacked a protocol for password changes after an employee leaves.
C. The system wasn't backed up.
D. The staff didn't understand how ePHI is lost.

10. One of your nurses and the office's physician assistant joked about a funny interaction with a patient on social media over the weekend. On Monday, you come into work, and there's an angry message and email from the patient, who saw the post. There were no photos and the patient was not mentioned directly by name. What happens next?

A. The nurse and physician assistant should be fired.
B. The post should be removed, and an apology should be issued to the patient.
C. Your compliance team should investigate if a HIPAA violation occurred.
D. All of the above.

Answer Key: 1. D 2. C 3. A 4. D 5. B 6. C 7. C 8. B 9. B 10. D.