Health Information Compliance Alert

Contingency Planning: Quiz Yourself on Disaster Protocol Basics

Tip: Ensure your staff know what to do, too.

Last year was one for the record books. Not only did providers have to figure out how to keep their practices afloat and care for patients in the midst of a pandemic, but they had to battle environmental and cybersecurity problems, too.

With lockdowns expected through much of 2021, it's a great time to review your contingency planning and update your compliance protocols accordingly.

Quiz your staff's contingency planning smarts with this quick question-and-answer set.

1. Are small practices really required to develop and document a contingency plan?

A. Yes, the HIPAA Security Rule mandates that all covered entities (CEs) have formal contingency plans for preparing for and responding to emergencies and other events that could damage health IT.

B. No, but it is considered a best practice.

C. No, but it may be a worthwhile effort.

D. Yes, but this is optional under the HIPAA Security Rule.

2. After Hurricane Sandy, the HHS Office of Inspector General (OIG) outlined five requirements that every contingency plan should have. Which of the following is not a requirement?

A. Critical assessment of all applications to address working order

B. A data back-up plan

C. A cloud infrastructure

D. A disaster strategy to recover lost health data

3. What HIPAA Security Rule requirement can help you identify problems, should be ongoing, and will help with contingency planning?

A. An office security system

B. A risk assessment

C. A business associate agreement

D. None of the above

4. What is something your staff should know before disaster strikes?

A. A communication strategy for operating without power

B. The written policies and procedures for EHR downtime

C. Which applications are critical to protect patients' data

D. All of the above

5. Name something your mobile device management protocols should address in your contingency planning.

A. Encryption

B. Remote logins and passwords

C. Multifactor authentication

D. All of the above

Answers: 1) A 2) C 3) B 4) D 5) D