Health Information Compliance Alert

Quiz: Discover How Much Your Staffers Know About Contingency Planning

Understand what is truly critical to your office operations.

A hurricane, a flood, a tornado do you and your staff know what to do when disaster strikes? Contingency planning is an essential process for protecting your data in the event of a natural or man-made disaster, even if it's simply a power outage.

If you and your staff want to test your contingency planning know-how, take the Contingency Planning Challenge (www.healthit.gov/providers-professionals/privacy-security-training-games), a fun and interactive game developed by the Office of the National Coordinator for Health IT (ONC). Here are a few sample quiz questions from the game:

1. How does having a Contingency Plan benefit our practice?

A. Planning can help our practice effectively protect and recover our revenue.
B. Planning can help our practice mitigate patient safety issues such as the difficulty of sending prescriptions to the pharmacy for high-risk patients.
C. Planning can help us protect, and if necessary, recover patient records.
D. All of the above.

2. We aren't located in a flood plain or where there are a lot of hurricanes. We don't have to worry about any other kinds of risks, do we?

A. No, you only have to plan to respond to natural disasters, like tornadoes, floods and wildfires.
B. Not if you have insurance.
C. No, why waste your time planning for something that is not likely to happen?
D. Yes, if you don't plan for threats like fire, vandalism or power outages, your information may be vulnerable to loss or damage.

3. We're a small practice. Are we really required to develop a Contingency Plan?

A. Yes, the HIPAA Security Rule requires a practice to have a formal Contingency Plan for preparing for and responding to emergencies and other events that could damage health IT systems.
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.

4. The office manager has asked me to help assign personnel roles and responsibilities in our Contingency Plan, because I know everyone in the office and what they do. What are some of the things I may need to consider?

A. Who needs access to ePHI in the event of a natural or man-made disaster?
B. Who should be responsible for implementing the Contingency Plan?
C. Who may need access to our office to help restore lost data?
D. All of the above.

5. Now that we've adopted an electronic health record (EHR), I'm worried about what we would do if anything happened to interfere with or damage our health information system. Planning ahead sounds like

a good idea. How can we learn more?

A. The HHS Office for Civil Rights (OCR) and the ONC websites provide information on how to prepare for natural or man-made disasters.
B. The National Institute of Standards and Technology (NIST), the federal agency that works with industry to develop and apply technology, measurements and standards, has information about developing a Contingency Plan on its website.
C. The Centers for Disease Control and Prevention (CDC) has information to assist healthcare providers in preparing for unplanned events including public health emergencies.
D. All of the above.

6. We're a small office, but we need to have a plan to back up data that is on our office computer server, so that it's available if something happens to our information system. What can we do to save and store data should something happen to the office?

A. Store the encrypted media in a secure location in the office and securely transport the encrypted media from the office to an alternative safe location on a regular basis. Include the process and location in your risk assessment.
B. Research and contract with an offsite hosting vendor that is HIPAA-compliant. Backups could then be scheduled to occur primarily during periods of lower activity.
C. Contact your IT/EHR vendor to discuss setting up a remote backup server that would permit staff to access files they would need on a daily basis from any location if the information on their primary server becomes inaccessible.
D. All of the above.

7. What are some of the procedures we need to include in our Contingency Plan?

A. Procedures for backing up patients' clinical and billing information.
B. Procedures for restoring any lost clinical or billing information.
C. Procedures that enable critical business processes for protection of the security of health information while operating in an emergency mode.
D. All of the above.

8. As we develop our Contingency Plan, what are some key things we may want to consider in order to develop an effective plan?

A. Ensure that you name an individual who is responsible for activating the plan and the individual understands his or her role.
B. Ensure the plan is updated when you hire new staff, purchase new IT hardware/software, or change locations.
C. Test the plan to make sure it works.
D. All of the above.

9. We need to assess what hardware and software is critical to our office operations, but everything we do seems so important. What is an example of critical software that we may need to protect during an emergency?

A. Our EHR, especially patients' medication lists.
B. Online medical journals, so we can stay up to date.
C. Free Wi-Fi for our patient waiting room.
D. Search engines so that we can stay up to date on the emergency.

10. We have a waiting room full of patients and the power has gone out. Apparently, the power is out due to a transformer fire and most of the city is affected. What should I do?

A. Send all of the patients home; there is nothing you can do.
B. Activate the Contingency Plan, which should: detail how to document visits when the EHR is unavailable; describe how the new information will be incorporated into the EHR when the power returns; and detail how to ensure that the data is safeguarded during the emergency.

C. Yell at the doctors for not agreeing to get a back-up generator when you suggested it.
D. Smile and hope that no one notices.

ANSWER KEY: 1. D 2. D 3. A 4. D 5. D 6. D 7. D 8. D 9. A 10. B.