Long-Term Care Survey Alert

HIPAA Awareness: Are Sure Your Residents' PHI Isn't in Jeopardy?

Disaster preparedness shouldn't leave loopholes that could sink your HIPAA compliance.

If your facility has recently switched to using a cloud-based electronic health record (EHR) as part of your contingency plan, you need to take certain precautions to guard against breaches. Don't get tripped up by this and other common compliance traps.

Think your contingency plan is rock-solid? Put your plan to the test with these questions from the **HHS Office of the National Coordinator for Health Information Technology's** (ONC) web-based privacy and security training modules (go to www.healthit.gov/providers-professionals/privacy-security-training-games).

1. We've completed our Contingency Plan. What should we do now?

A. Mission accomplished! You are now safe from all disasters.
B. Regularly review the plan to see if you need to update it to reflect changes to your staffing, information systems, or office location.
C. Have a meeting and tell everyone what the plan is. No need to provide a copy.
D. Keep a copy of the plan on your computer and tell everyone where to find it.

2. We use a cloud-based EHR which can back up our facility's information offsite. What else do we need to do?

A. Under the HIPAA Security Rule, regardless of where you store your information, you must have a written Contingency Plan to effectively safeguard the confidentiality, integrity, and availability of ePHI.
B. If your EHR vendor will be backing up your information, you should have a formal agreement including a Business Associate Agreement, that specifically details the procedures for you to access your ePHI in case of network interruption.
C. You also need to have procedures in place to ensure data is restored quickly, reliably, and securely.
D. All of the above.

3. It's been a while since our facility has looked at our Contingency Plan that was developed more than a year ago. How often should we review and update our plan?

A. We never review it after we develop it. We're done!
B. We have a lot of staff turnover. We should probably review and update our plan periodically or after a significant change to our environment.
C. We are going to wait and see how this current plan works during an emergency event; then we will review and update our Contingency Plan.
D. We haven't heard of any recent HIPAA audits by HHS, so no need to update it yet. I'll send a reminder email to the office manager to consider this in the future.

4. We never tested our EHR data backups. Now I can't retrieve patient information that appears to be lost after an application upgrade. What do I do now?

A. Find out if anyone has backed up the EHR on tapes or disc drives.
B. Contact your EHR vendor to request assistance in rolling back the upgrade or recovering as much of the database as possible from backup media starting with the most recent data.
C. Re-boot your server; this typically will resolve the problem and your EHR data will be recovered.
D. Try to recover from a previous backup; the data should not have changed very much.

5. We just discovered that one of our nurses has been viewing her estranged mother-in-law's EHRs and was sharing the

information with her friends. This is a violation of the Confidentiality Agreement that she signs annually and she will be terminated today. What should my next step(s) be?

A. Speak to the nurse and fire her immediately regardless of patients or other staff in the vicinity.
B. Call the nurse into your office prior to lunch and advise her that her employment is ceasing immediately. Make a note to notify tech support by the end of the week.
C. Contact the person with administrative privileges to deactivate all of her user accounts. Then, notify the nurse in private of her immediate termination.
D. Tell the billing manager to notify the nurse that she's been fired. Then, leave for a long lunch since you avoid conflict whenever possible.

6. The providers at our facility have decided they would like to use tablets to view health records, so we need to implement a wireless network. How secure does the wireless network need to be?

A. Ensure the facility's purchased router meets the necessary level of encryption.
B. Since it's such a small town, using WEP is fine. At least the wireless access point is secured.
C. Don't worry about encryption. The wireless range outside the facility is limited, so very few people will even notice the network exists.
D. Inform the providers that wireless networks cannot be secured so they should continue using their current wired local area network.

7. I've been noticing different things happening on the computers here in the office. For example, some people are getting a lot of spam. I suspect that one person is sharing her password with others. Also, several people have been talking about some gaming website they have been visiting during their lunch break. What should I do?

A. Contact other facilities in your area and informally survey them to see what practices they use.
B. Ignore the problem as long as it doesn't affect you.
C. Complain at the next staff meeting about people who share their password and use the Internet improperly.
D. Contact/hire tech support to perform a security audit.

ANSWER KEY: 1. B 2. D 3. B 4. B 5. C 6. A 7. D