Health Information Compliance Alert

Quiz: Test Your HIPAA Knowledge With This Quick Quiz

What's the first step in securing your office's network and hardware infrastructure?

How much does your staff really know about HIPAA privacy and security? Find out by giving them a fun quiz the **HHS Office of the National Coordinator for Health Information Technology** (ONC) has web-based privacy and security training modules in the form of games and quizzes (go to www.healthit.gov/providers-professionals/privacy-security-training-games).

Here's a sample of the quiz questions contained in the modules:

1. Physician: We are updating our technology and need to replace three old computers. After the new computers have been configured, what will happen to the old ones?

a) Take the old computers to the recycling center.

b) Install the new operating system and sell the old computers to employees for personal use.

c) Leave them on a shelf in the office in case someone needs to use the old computers.

d) Remove the hard drives and either destroy or wipe them to permanently remove all data prior to disposal.

2. Front desk clerk to billing clerk: I have a patient on hold and my password isn't working. Can I borrow yours?

a) Sorry, I cannot share my password with anyone. Let me help the patient while you call tech support.

b) No, but I'll log on with my password and you can take over from there.

c) Sure, no problem. Just don't tell anyone my password. Between you and me, you can use it as a backup anytime.

d) I don't see why not. You've signed our Confidentiality Statement and you have access to all the same information as I do.

3. Patient: I would like to bring by a USB drive to put my health records on. What time can I bring it over and how long will it take?

a) It takes five business days to get records. Using a USB drive does not allow us to get your records to you faster.

b) We cannot put records on a USB drive. You can only get printed records.

c) You can bring the USB drive over today and I'll check to find out if we can do that. No one has made this request before.

d) I'm sorry, we cannot use outside devices on our computers. We can provide you with your patient data on a USB drive that our practice provides. This USB drive can be picked up after three business days.

4. Billing clerk to office manager: Can I take my laptop home tonight so I can get caught up on billing for last week? I'm way behind. When I did that last time it really helped me to catch up.

a) Sorry, no computers with unencrypted patient information can leave the building. Let's talk with tech support to get

the laptop encrypted.

b) Let me think about it and weigh the pros and cons. I'll let you know after lunch.

c) Sure, the laptop is covered under our office insurance policy. Just be careful with it.

d) It's up to you. It is your responsibility if anything happens to that laptop.

5. Physician to office manager: I just got a call from another physician who is at a local medical conference and he wants me to email Mr. Lee's lab results to his personal email account. He plans to access the results from the hotel's business center computer. He's leaving the conference now to meet the patient at the emergency room. What should I do?

a) Reassure him you're on it. Email the record right away before you forget. He's a trusted colleague.

b) Determine if he has access to encrypted email and if not, request that our office staff securely fax the results immediately to the hospital labeled "Attn: Dr. Jones."

c) Knowing that he has a password on his personal email account, agree to send Mr. Lee's lab results. It will be safe enough and you know him well.

d) Do not tell anyone but go ahead and send the results anyway in this case. Chances are slim anything will happen.

6. IT sales rep to office manager: I'm the sales rep for your computer workstations and we have new software that will help your office secure your records. May I access a few patient records so I can show you how easy it is to convert to our new system?

a) You know this sales rep and have dealt with him before. You can trust him with the records, so you allow it.

b) Allow access to records of former patients so that no current medical information is compromised.

c) Refuse access to your patients' records and request a demonstration using test data.

d) Refuse access to patient records but offer records of the office staff from whom you have permission.

7. Physician: After calling the nurse out for a quick consultation, I found her tablet in the examination room with the patient, unattended. What should I do first?

a) Play it off as insignificant by asking the patient, "What level of the Angry Birds game are you on?"

b) Have someone run an audit trail report to determine if any PHI was inappropriately accessed.

c) Bring the nurse into the room and chastise her so the patient can see you are taking the incident seriously.

d) As soon as you have finished the patient visit, pull the nurse into the office manager's office and berate her for her thoughtlessness.

8. Front desk clerk: My laptop was stolen out of my car last night and I don't think it was encrypted. I took the laptop home because I thought I'd try to learn the new billing software on my own. So because of me, a lot of patient data may now be breached. What does the practice do now?

a) Conduct an investigation to determine if patient data was breached. If yes, identify state and federal laws that apply, notify patients of the incident, and provide appropriate resources.

b) Establish a new internal procedure with training requiring that all new mobile devices are encrypted before they are given to employees.

c) Take disciplinary action on the employee at fault to ensure that she understands the seriousness of the breach.

d) All of the above.

9. Physician: At a conference, I learned about the importance of securing the network and hardware infrastructure in my office. I know what I should do next!

a) Research network security in order to select and implement the best configurations for the needs of

the office.

b) Buy the hardware and/or software to secure your network and ask around for someone willing to do the installation.

c) Hire technical support to assess your current network configuration, recommend and explain upgrades/improvements, and secure your network.

d) Assign an office staff member to secure your network.

10. Physician to office manager: In the last few years, we have had a couple of hurricanes that caused a lot of flooding. What steps should we take to back up our computers and patient data?

a) Install a fireproof, permanent safe at the physician's home. He lives right around the corner, so that should be convenient.

b) Have fireproof portable boxes with the backup data hidden at the office.

c) Make paper copies of all the records and place them in a storage unit.

d) Backup your PHI on an encrypted media device and secure it at an alternate facility.

ANSWER KEY: 1. d 2. a 3. d 4. a 5. b 6. c 7. b 8. d 9. c 10. d.