Health Information Compliance Alert

SECURITY QUIZ: 6 Simple Questions Will Jumpstart Your Compliance Engines

Just when you were feeling confident about the state of your privacy rule compliance, the feds throw the security rule at your feet. But don't fret, covered entities: Eli provides you with all of the answers!

You've been diligent with privacy rule compliance, and you're ready for the next hurdle. Now ponder these six questions and then sit back as **Jennifer Bever**, a consultant with Chicago-based **KarenZupko Associates**, walks you through the answers:

Question 1: Are there physical barriers to prevent patients/visitors from viewing computer screens?

Answer: Bever says there are many CEs out there that are concerned they'll have to build new walls and close off front desk windows, but she tells **Eli** there are some low-cost solutions to this problem. For example, here's what to do if your organization has several computer terminals in an area where a patient could walk through and see them.

"We'd like to see a basic screen saver that locks out after some period of no motion on the keyboard or the mouse" Bever advises. She says if a staff member walks away from his desk, the computer should shut down after 30 seconds of inactivity. "That way, whoever's walking by when you're away from your desk can't see anything they shouldn't."

Also, Bever has observed that front desks at physician's offices and hospitals often have computer screens that are somewhat visible by patients. When that happens, ask yourself if the patient can view things on the monitor he shouldn't see. If a patient is sitting over in the waiting room at an angle where he can see the computers, you can buy a special type of screen cover for your computer, she notes. It lays flat against the computer screen, and if someone looks at the screen straight on, he can see everything normally, but if he looks at it from an angle - if a patient is passing by or is seated off to the side - he wouldn't be able to see anything. And that's the type of simple, cheap device you can purchase at most office supply stores. "It's not exorbitant. If you had 20 computers, it would be pretty reasonable to buy those for your front desk folks," she maintains.

Question 2: Do you limit access to data by job function?

Answer: Not all staff members require the same access to your systems. What you need to do, Bever suggests, is to pull up the job description of everyone in your organization. After reading the job description, ask yourself, "Based on what I know this person does in day-to-day performance, she needs access to the following systems to do her job." Bever says access should be based on a case-by-case basis.

In a physician's office, most staff members are cross-trained and perform several different tasks, so in that case one can make an argument that most of the staff will need access to most of the systems. Conversely, if you're a nurse you would clearly need access to an electronic medical record, but would you need access to the patient's financial records? "Probably not," says Bever. "Really, you have to go by job type and ask what kind of information would each staff member require," she explains.

Question 3: Can you audit employees' access to data?

Answer: For the most part, computer systems leave footprints, Bever maintains. "Whoever you are, you sign in to the system and you leave footprints around the system." This is something with which most CEs are not familiar, and Bever says you might have to rely on an IT professional to determine what types of data an employee has viewed. If you find out that someone was in an inappropriate data set, you'll have to develop some method of how you respond to certain

inappropriate actions. "I think that's a pretty big black hole for entities right now," she says. Make sure you develop a set of policies that explains what you'll do if push comes to shove and you must discipline an employee who views data he shouldn't have.

Question 4: Does your system have a firewall in between the internal system and the Internet?

Answer: Many CEs have staff members up on the Internet and receiving emails all day, and both of those make internal systems susceptible to hackers and virus. "To have online access in email and not have a virus protector and a firewall is asking for trouble," Bever warns. Odds are that you're already using some anti-virus software, but you might not have a firewall in place. "Think of a fire-wall as a physical wall that allows certain data to enter your system while prohibiting other data from entering." If you don't have a large IT department in your organization, don't worry. If small CEs don't have the resources to hire an IT professional, try outside help. Bever says there are firms that deal with issues exactly like this one that run help desks. You can simply sign up and they'll be your troubleshooter, so when you need help with small issues like this, they can serve as your outsource support.

Question 5: Is confidential (containing PHI) e-mail encrypted?

Answer: Bever says she was shocked that HHS failed to mandate email encryption, considering the high number of email breaches she's witnessed. If hackers really want to, they can break into your everyday e-mail correspondence anytime. If you're not willing to tolerate that risk, there are practical and easy solutions you can utilize.

For instance, take a peek at **Medem.com**, a Web site that focuses on secure doctor-patient email communications. Medem's Online Consultation is a tool that allows physicians to securely communicate online with patients and receive payment for their work by providing physician offices secure communications with patients, other providers, their hospitals and others. Bever says Medem has a set up where a physician can create a Web site through Medem or they can use an online consultation feature in conjunction with their own Web site.

Here's how works: The patient e-mails to the physician but it travels first to Medem's database. The physician is sent an e-mail that asks him to check the database for a new message. Then the physician goes into the database and signs in with a password, checks the e-mail and responds. The patient does the same thing, so the messages don't travel over the Internet to each other in unencrypted form; they go into a database that you then tap into, and you can read the confidential info there.

Question 6: Is there a written protocol in place to protect data/systems when an employee leaves the practice?

Answer: This should be done after you create a list detailing what kind of access each staff member has. When staff first accept a position at your CE, there needs to be a checklist given to the new employee in which he checks off all the items given to him, including all the keys and passwords needed for him to do his job. That way, when the employee leaves, you can pull out the list and check off all the items listed.

This is especially important if an employee is being terminated for cause. If that's the case, Bever says she'd "probably be in a heightened state of emergency that computer password issues are taken care of before [the employee] leaves the building." Bever says she knew of an employee who was about to get fired. The employee started emailing financial information of the practice's network to a colleague, as well as different forms that the practice used. "She mailed it out and they caught her. Before she was actually fired, someone checked her computer and her email to see what kind of activity had been going on there. When she came in the next morning, the doctor, the administrator, and the attorney were there. People need to take this stuff seriously," she admonishes.

Editor's Note: This questions included in this quiz were created by Jennifer Bever and Larry Bossom. The latter works as a senior project manager for Project Leadership Associates in Chicago.