Codify
BY AAPC

Health Information Compliance Alert

Security Strategies: Check Your Security Plan For These Safety Measures

Visitors could be downloading PHI right under your nose.

Safeguarding your practice from security breaches may be as simple as posting rules about camera phones, but have you done this yet? Experts offer three "no's" to help stop PHI thieves in their tracks.

No Technological Safe Zones

As advanced technology becomes more available, we've begun to see interesting phenomena -- like camera phones -- that allow users to take information with them.

Caution: This is a wolf in sheep's clothing; these advancements give users the ability to manipulate security measures without breaking a sweat, experts say. Camera phones, PDAs and Blackberries, among others, are high-risk media because users can take pictures or upload information such as PHI right from under a hospital's nose, states **Kerry Kearney,** a partner at **Reed Smith** in Pittsburgh. And "there's nothing about a hospital's administration that can go to the level of banning people" from having these devices inside your facility, she laments.

Best Policy: "It is difficult to ban them, but you could post rules that say no photo phones are allowed," suggests **C. Jon Burke,** a California-based data security specialist for **Toshiba American MRI** and **Toshiba American Medical Systems.** Though the rule would most likely be broken, at least your facility will have a policy in place if that broken rule leads to a security breach, he says.

"Certainly you can regulate the use of [these devices] by employees and contractors," Kearney reminds. "Employees should be required to use technology responsibly," she says.

Example: The worst-case scenario is that your facility waits until it's too late to develop, distribute and enforce policies and procedures to control these types of devices. One hospital, which discovered its union workers were using camera phones to record working conditions, implemented a camera phone policy after the damage was done, Burke offers.

"They were not allowed to implement the policy because it now impeded an investigation," Burke says.

Tip: While you may not be worried about heading off an investigation, you should worry about the ramifications of your patients' PHI leaving the hospital via pictures or other media, experts counsel.

No Floating Calendar

Do not fall into the procrastination trap! "Time is going to sneak up on you," warns **William Hubbartt,** president of St. Charles, IL-based **Hubbartt & Associates**.

Remember: The sense of confidence instilled by facilities' privacy rule work could lull you into believing you've got all the time in the world to implement your security measures. "There's a better feel for what needs to be done for security now that privacy is done," but that could back-fire, Hubbartt says. In the aftermath of the big privacy rule push, many organizations think they've done enough, he notes.

Warning: "That 'head in the sand' approach is a huge threat" to your security rule compliance, Hubbartt stresses. Just like the privacy rule, the security rule "necessitates taking time and effort to write selected policies, procedures and forms - and enforcing them," he says.

And because many of the standards are commonplace for those facilities with skilled, experienced information technology staff, the tendency is to put the security rule on the back burner. However, security rule compliance is not to be taken lightly, as penalties can crush facilities faster than natural disasters.

No Miscalculations

The security rule, while not as mystifying as the privacy rule, is similar to the latter in that "most of the time what we're up against are mistakes," Burke explains.

Reality: "Very few people [violate] HIPAA to be cruel or for profit," and so the more time and effort medical facilities spend ensuring their security rule compliance, the less likely it is that crucial mistakes could lead to a HIPAA violation, Burke says.

Strategy: "The key is to not underestimate the security rule's importance," Hubbartt declares. By understanding this importance, and taking all the measures you can to facilitate your organization's security, "you'll save yourself time and money in the long run," Burke asserts.