Long-Term Care Survey Alert

Medical Privacy: Don't Let Your Facility Be Toppled by HIPAA Noncompliance: Perform a Topnotch Security Risk Analysis

Beware 'willful neglect' penalties up to $50,000 per violation now in effect.

If you think survey CMPs add up fast, take a look at the fines associated with "willful neglect" HIPAA violations, a category that went into effect on Feb. 17.

Ouch: If HHS determines a willful neglect violation occurred, which essentially means you didn't identify and try to preempt the risk -- you can get hit with fines starting at $10,000 per violation, says HIPAA compliance expert **Jim Sheldon-Dean.** "And that's if you correct the problem within 30 days," he adds.

"If a provider takes more than 30 days to correct the violation, then the fines start at $50,000 per violation," adds Sheldon-Dean, principal and director of compliance

services for Lewis Creek Systems in Charlotte, Vt. (The HITECH Act implemented the heftier fines for HIPAA privacy and security violations in February 2009, he notes.)

It gets worse: Sometimes one problem gets counted as multiple violations, each one ringing up a stiff fine. The number of violations "can multiply very quickly," says Sheldon-Dean.

Who might report a willful neglect violation? Most frequently, an employee who's been mistreated or terminated files such a complaint against the employer, says consultant **Abner Weintraub,** based on his experience as an expert witness in HIPAA cases. The second most common scenario involves a patient filing a complaint, which in a nursing home might be the family member filing a complaint on the patient's behalf, adds Weintraub, president of The HIPAA Group Inc. in Orlando, Fla.

Nail Down the Essentials for Doing a Risk Analysis

You can, however, stave off crippling fines by performing a thorough HIPAA risk security analysis in order to comply with the security rule, if you haven't already.

As a first step, a provider or other covered entity has to do a risk analysis, says Sheldon-Dean. The analysis focuses on looking at the "big picture" to identify potential risk points, he says.

Start by identifying what systems are holding onto electronic health information that contains PHI, including electronic health records and business files, Sheldon-Dean advises. "Look at how those systems move information within the entity, as well as to business associates outside the entity or to other entities for other purposes."

After identifying the risk points, do a more detailed risk assessment of your individual systems. You identify their specific risk points, as well as significance -- and the likelihood that a problem will occur, and then address it, Sheldon-Dean instructs.

There are several ways to do the risk analysis assessment, he adds, but the simplest approach is to use a methodology defined by the National Institute of Standards and Technology special publication on risk analysis (http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf).

Target These 2 High Risk Areas

Some of the riskiest areas these days involve portable devices containing protected health information, warns Sheldon-

Dean.

Little devices, big risks: "As devices get smaller and more portable, the potential for lost or stolen or misplaced data increases -- and so does the risk for a breach," warns **Peter Arbuthnot, RAC-CT,** regulatory analyst with American HealthTech in Jacksonville, Miss.

In fact, identity thieves view health information data as the "highest quality" available for their purposes, warns Sheldon-Dean.

Must do: "It's really important to secure the information on devices by encrypting it and also have the capability to remotely wipe the devices clean, including laptops," he advises. To accomplish the latter, you set the device so that the next time it's turned on, the device calls home over the Internet, Sheldon-Dean explains. Then the software can tell the device "you've been stolen," which causes the device to eliminate its data.

Unsecured e-mail is also high risk, says Sheldon-Dean. "Copies can be left on mail servers or in unsecured areas."

Solution: Based on the HITECH Act, says Sheldon-Dean, the proper ways to secure e-mail or other documents/systems/files/data are defined in guidance from HHS, available at: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html.

Key: "If electronic data has been secured (encrypted), then the covered entity does not have to report a breach," says Weintraub. "The assumption is that properly encrypted data is useless to anyone who has it."

Watch Out for Remote Access

Remote access is another high-risk issue for facilities that have staff or contractors who use computerized PHI offsite, says Sheldon-Dean.

For one, "the PHI may end up on networks or computers that aren't properly secured," he cautions. Or an employee's family members may view the information when they use the same computer. "Even if you make the remote connection secure, once the data is on someone else's computer -- it's outside the facility."

To avoid these risks, the facility can develop policies forbidding people offsite from accessing confidential information, says Sheldon-Dean. If someone has to work from home, the facility can provide the person with a dedicated computer. And you can set it up so the person accesses data over the web securely without being able to save or print the information, he adds.

"You can use something like Citrix to tunnel into the entity's systems and work on them remotely without actually bringing any persistent data into your remote computer," explains Sheldon-Dean.

That way, "you don't wind up with any temporary files on the remote machine."

Don't Forget to Audit

Skimping on the audit process can be a costly mistake. You have to make sure everyone is doing what's expected based on policies and procedures, including managing risks related to portable devices and remote access, says Sheldon-Dean.

Remember: The HITECH Act requires HHS to conduct random audits of various types of entities, he says. And whatever fines HHS collects from the audits will go intoan audit fund to pay for additional audits. Thus, "once HHS gets going, the audits will ramp up quickly."