Codify
BY AAPC

Health Information Compliance Alert

Risk Management: Don't Be Toppled by Giant Fines: Perform a Topnotch HIPAA Security Risk Analysis

Beware: The willful neglect category of violations goes into effect on Feb. 17.

If you've put off doing a thorough HIPAA security risk analysis, you have a compelling reason to do so now -- and quickly.

Watch out: The willful neglect violation category kicks in on Feb. 17, 2011, says **Jim-Sheldon Dean,** principal and director of compliance services for Lewis Creek Systems LLC in Charlotte, Vt. Willful neglect means a violation occurred because the provider or other covered entity didn't pay attention to the rules and do the work necessary to prevent the problem, he explains.

A patient might report such a violation if he sees shortfalls in privacy or security at your practice -- or suffers a privacy breach as a result, says Sheldon-Dean. Or a disgruntled employee could turn in his employer for non-compliance.

Bottom line: HHS has to look into such reports. And if the agency determines a willful neglect violation occurred, it must impose fines starting at $10,000 per violation -- and that's if the provider corrects the problem within 30 days, Sheldon-Dean says. "If the provider takes more than 30 days to correct the violation, then the fines start at $50,000 per violation." (The HITECH Act implemented the heftier fines for HIPAA privacy and security violations in February 2009, he adds.)

It gets worse: Sometimes one problem gets counted as multiple violations, with each one ringing up a stiff fine. And the number of violations "can multiply very easily," Sheldon-Dean cautions.

Nail Down the Essentials for Doing a Risk Analysis

As a first step in complying with the HIPAA security rule, a provider or other covered entity has to do a risk analysis. The analysis focuses on looking at the "big picture" to identify potential risk points, says Sheldon-Dean. You start by identifying what systems are holding onto electronic health information that contains PHI, including electronic health records and business files.

"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," Sheldon-Dean advises.

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, Sheldon-Dean instructs.

There are several ways to do that, 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).

Know the Score

Using that methodology, you look at each identified risk and consider how big of an impact it would have if something went wrong, he advises. "For example, the potential impact will be higher where you have a higher number of individual records or ones with greater details." Rank the impact on a scale of 1 to 3 (low, medium, or high).

Next, "look at the likelihood of this risk actually becoming an issue," and rank that 1 to 3, as well. Sheldon-Dean advises.

What might warrant a high score in terms of being likely to happen? One example would be a problem that an or a

similar entity one has already experienced but hasn't taken steps to help prevent, he says. If you don't reasonably believe an issue could occur, assign ita low score.

Next: Multiply the impact score by the likelihood score, which gives you a risk score, Sheldon-Dean explains. "You'd deal with any risk scored as nine first. Risks with a score of six would also be higher priority."

Even risks with a lower score might also deserve immediate action if they are inexpensive or easy to address, he points out. While the risk numbers help you prioritize, you should consider them "in the context of a limited budget and time. Don't ignore easy fixes because they aren't as high risk as some others."

Watch out: Some of the riskiest areas these days involve portable devices or portable media, and remote access, warns Sheldon-Dean. (For details and the latest strategies to help risk-proof these problems, see the next Health Information Compliance Alert.)

Remember: Assessing and addressing risks isn't a onetime deal. Instead, stresses Sheldon-Dean, "it's a neverending process."

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, urges he.

Beat HHS to the punch: "It's better to audit yourself before HHS comes along and does an audit or the local news station reports on a breach" at your organization, he points out.

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

Keep in mind: Providers also have to do a HIPAA security risk analysis to be eligible for Medicare or Medicaid electronic health record incentive dollars, advises Sheldon-Dean.