Health Information Compliance Alert

What Constitutes a Violation? Find Out

Get your ducks in a row with a clear-cut explanation before you make the call to HHS.

Before you can start identifying potential breaches at your practice, it's important to know what the law says. Particularly with a breach like that of the Aetna case, where the PHI exposure of delicate information has already begun to wreak havoc on people's lives.

Take a look at this handy go-to guide for review before you call the HHS-OCR to report a HIPAA violation.

"According to the Privacy Rule, a breach is any acquisition, access, use, or disclosure in violation in the privacy rule and that covers a lot," says **Jim Sheldon-Dean**, director of compliance services with Lewis Creek Systems, LLC in Charlotte, Vermont.

Nuts and bolts: However, there are exceptions under which you aren't required to report the breach, including the following, he adds:

- **If the data is destroyed or secured according to HHS guidance.** "Make sure you use good-quality, secure encryption," he cautions.
- **Unintentional internal use, in good faith.** For instance, if you put a folder on the wrong desk and a physician opens it, says, "Oh, these aren'tmy patient's notes, these belong to someone else" and closes it, you aren't required to report that.
- **Inadvertent internal use, within job scope.** For example, someone looks up the records for Mary Smith but opens the notes for the wrong Mary Smith, realizes her mistake, and then closes out the notes.
- **Information cannot be retained.** For instance, you lose a box of medical records and you find them the next day with the box still sealed the way you left them, and you know the information was not breached.

If you don't meet these exceptions but you can prove there was a low probability of compromise based on your risk assessment, you may still be in the clear, Sheldon-Dean says. The risk assessment must include a detailing of what information was in the records, how well-identified the PHI was, and whether its release would be "adverse to the individual." You'll also have to assess to whom it was disclosed, whether it was actually acquired or viewed, and the extent of mitigation.

Scenario: Suppose you fax an allergy test result with just patient initials to the wrong physician. The physician calls you and says, "You meant to send this to someone else, we're shredding it." That's a low probability of compromise, with very little identifying patient information on it, Sheldon-Dean maintains.

Don't Forget to Analyze Your Assessment Data

Whenever you do a risk analysis, remember that each risk issue has an impact and a likelihood, he notes.

Repercussion: The impact refers to how great the damage would be a lot of information about a lot of people with excessive detail would have a greater impact.

Probability: Likelihood refers to how likely it is that the risk issue would become a reality.

Once you analyze your practice's risk, if you find breaches to report, don't just tell the government, "We had a breach." Instead, say, "We had a breach, we know what happened, we fixed the problem, we've had some improved training, policies and procedures, we've done some auditing to make sure everything is better, and you'll never hear about this problem from us ever again." If you include that type of information with your report, they'll be less likely to ask further

questions, Sheldon-Dean advises.