Long-Term Care Survey Alert

HIPAA: Follow the Ins and Outs of Finalized Breach Notification Rules

If a breach involves 500+ people, here's what your facility will suffer.

Picture this: A nurse hands a patient someone else's discharge papers but promptly discovers the error and retrieves the protected health information. Would your facility have to report that as a breach of unsecured PHI under HIPAA notification rules that went into effect on Sept. 23?

The answer: It depends. The scenario wouldn't constitute a breach -- "if the nurse can reasonably conclude that the patient couldn't have read or otherwise retained the information," according to the Health & Human Services' (HHS) interim final rule implementing the new requirements. But suppose the patient turned the corner and was out of sight momentarily and the discharge orders included "a sensitive diagnosis such as HIV, and the facility was in a small community"-- or the nurse had reviewed the discharge orders with the patient, says Chicago attorney **Michael Roach.** Those scenarios could trigger the notification requirements, he points out.

Nail Down the Basics

The notification requirements, which are required by the economic stimulus bill's HITECH act, apply to a breach of unsecured PHI that poses a significant risk of financial, reputational or other harm to the affected individual. Securing electronic PHI requires encryption that meets HHS' specified standards, says Roach. You can't, of course, secure PHI in paper records. The rule does, however, discuss "rendering PHI in paper records as unusable," when the records are no longer needed. Most people seem to be interpreting this as requiring "cross-hash-shredding or incineration," Roach notes.

Good and very bad news: The rule allows your nursing home and other covered entities to determine whether a breach of unsecured PHI poses significant risk of harm to the affected individual(s). If you determine that it doesn't pose such a risk, then you don't have to report it. The risk analysis "is a change in the regulation based on what's in the HITECH law," observes **Jim Sheldon-**

Dean, principal and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vt. Conversely, if you do determine that a breach poses a significant threat, the facility has to notify the affected individual or individuals. In addition, "if the breach of unsecured PHI involves more than 500 individuals in any jurisdiction, then the facility [also] has to notify HHS and the media," says Sheldon-Dean.

Not only that, but "the facility will end up on the HHS' wall of shame on its Web site," he adds. If the breach involves more than 10 individuals for whom the facility has no contact information, "you may need to post a notice on your Web site or notify the media, providing a toll-free telephone number" for people to call.

Know How to Perform a Proper Risk Analysis

The facility should do a careful analysis to determine whether a breach of unsecured PHI triggers the notification requirements, Roach advises. For starters, take a look at whether the breach fits an exception. Three of these "appear to be intended to cover basic problems encountered in normal work situations," says attorney **Kathryn Solley,** with the Atlanta law firm Seyfarth Shaw LLP.

Note: For a quick rundown of the exceptions, see the sidebar on page 87 of this issue. The risk analysis will differ depending on what happened, as Roach points out in the scenario at the beginning of the article where a nurse gives a patient someone else's discharge papers.

Example: Suppose someone lost a piece of paper with a list of hospital patient names without any other identifying

information. "That might not be viewed as posing risk of significant harm, as it just tells you that the people came in for an appointment of some sort," Sheldon-Dean says. But a list of names of people in a nursing home might be another story. Identity thieves "might capitalize on that information, or it might tell them that the person isn't at home," he cautions. If the facility's team decides a breach doesn't require notification based on the rule, make sure to ocument how and why it arrived at that conclusion. "The issue could come back years later," Roach warns, "and if the facility doesn't have good documentation of the analysis, people will have to rely on their memories." Roach notes that "the government may disagree with the facility's conclusion but at least the analysis shows the facility acted in good faith.

That's one of the top things we advise people to do."

Remember: Even if the federal law doesn't require notification, the state law may, Roach reminds. "Most states have some sort of health information breach notification requirement," he says.