Codify
BY AAPC

Health Information Compliance Alert

The Third Degree: READER QUESTIONS ANSWERED

A HIPAA CHAIN OF COMMAND?

We're a large hospital and but we have employed a HIPAA privacy officer only so far (no security officer). We're strongly considering hiring a security officer to coordinate and manage our IT systems and to implement our security rule compliance plan. How should the security officer work with the privacy officer? Will the security officer report to the privacy officer, or do they work in tandem and report to someone else (an Executive VP or CEO)?

- Utah Subscriber

"I think the security officer should be on the same level as the privacy officer," says **Kevin Beaver, CISSP**, president of information technology and security consulting firm **Principle Logic** in Atlanta.

Beaver says both positions are equally important and believes that both the privacy and security officers would likely report to the organization's CIO, CMO, or CEO. No matter what, though, wherever they're positioned in the organization, your security officer needs to have the utmost decision making authority when it comes to security related issues. "When a network is attacked by a hacker or a data center is destroyed, there's no time for micromanagement or egos. The security officer just needs to be able to respond quickly and make important decisions on behalf of upper management," he urges.

EMPLOYEES AS PATIENTS UNDER HIPAA

How should a medical facility handle employees' access to their own medical records? That is, should employees within a medical center or practice who have PHI on the facility's computer system be able to view their own PHI?

- California Subscriber

"Everybody has access rights under HIPAA," reminds **Robyn Meinhardt**, an attorney in the Denver office of **Foley & Lardner**. Meinhardt says she's aware of some facilities with electronic medical records that have allowed their health care provider employees to access their own records with minimal interference from the system. In other words, if the employee inputs his Social Security Number, that'll give him access to his own PHI.

Meinhardt says one way to prevent employees from gaining easy access to their records would be to make them go through the normal access procedures, just like any other patient would have to go through.
The question that arises is, "Can you make it easier on employees to see their own records than for other patients?" Meinhardt says there may be some prohibitions under state law that might come into play here. "If your state law contains a prior physician review requirement, that could prevent an employee from gaining easy access to his records," she notes. But Meinhardt says it's likely - though not definite - that HIPAA would preempt the state law if that state law imposes a prior physician review requirement, so you should review your state laws to determine how they approach this requirement.

The Bottom Line: There's nothing wrong with a medical facility requiring the same access procedures for employees as it does for all other patients.

SET TRAINEES STRAIGHT WITH PHI

We're an academic medical center and we must routinely teach our medical students and trainees about HIPAA's privacy rule and how they must safeguard PHI. What do you think is the most important piece of information to impart to students about HIPAA who are just being introduced to patient privacy?

- New York Subscriber

"The thing we were most concerned about was students taking PHI from a training setting and disclosing it back in a classroom," says **Rebecca Hutton**, privacy officer at the **University of Wisconsin - Madison**. "That's what we were trying to emphasize the most - that [students] could not use identifiable information except in the training setting."

Hutton says sometimes students would bring protected health information back from a training site and disclose it among classmates for, say, a class presentation. So, informing students of their responsibilities with PHI was of grave concern to her and other professionals at UW.

Additionally, Hutton tells **Eli** that students often have trouble de-identifying PHI. "If you look at what you have to do to de-identify PHI under HIPAA, not all of that is really intuitive and identifiers can easily slip out in a conversation."

Tip: Make sure you provide your trainees with a list of the 18 identifiers that make up an individual's PHI. You can download the list at www.hhs.gov/ocr/combinedrules.pdf on pp. 29-30. And be sure to take the HIPAA Identifier quiz in this issue!