Health Information Compliance Alert

Security Strategies: You Be The Security Officer: Do We Have To Report All Employee Contact With Patients' PHI?

Read the situation below and decide how you would handle it before you compare it to our expert's advice.

Question: A patient requested that we account for all disclosures of her protected health information (PHI). Does the privacy rule require us to provide her with the names of each employee who accessed her medical information?

Answer: No, says **Kelley Meeusen,** privacy officer for **Harrison Hospital** in Bremerton, WA. "HIPAA created a clear distinction between 'uses' and 'disclosures,'" and internal employee access is most likely a 'use,' he explains.

A disclosure is when a patient's medical information is released to a person or entity outside of your organization, Meeusen says. On the other hand, patient information shared within your office to facilitate patient treatment is a use (Section 164.510), he asserts.

Use this quick guide to know which medical information sharing you don't have to track in patients' accounting of disclosures:

□□ Disclosures for treatment, payment and health care operations (TPO);

□□ Disclosures to the subject individual;

□□ Incidental disclosures;

□□ Disclosures the individual authorized;

□□ Disclosures for national security or intelligence;

□□ Disclosures to correctional institutions or law enforcers;

□□ Disclosures that are part of a limited data set; and

□□ Disclosures that occurred prior to the compliance date for the organization.

The bottom line: The privacy rule allows you to share information as necessary to ensure the best treatment for your patients, Meeusen says. **Remember:** If you catch an employee snooping in a patient's medical records for reasons other than treatment, you do have to account for that disclosure.