Codify by AAPC

MDS Alert

Privacy Compliance: Take a Hard Look at Whether Your Facility Is Vulnerable to This HIPAA Violation

If your staff ever carries paper PHI offsite, implement these proactive strategies.

HIPAA enforcement is heating up, and you don't want your nursing facility organization to end up forking over a million-dollar fine due to an accidental breach.

That's what a Massachusetts academic medical center had to do recently when an employee lost paper PHI that she took offsite for work purposes.

What happened: According to the medical center's resolution agreement with the HHS Office of Civil Rights (OCR), an employee "while commuting to work on the subway ... removed the documents containing PHI from her bag and placed them on the seat beside her. The documents were not in an envelope and were bound with a rubber band. Upon exiting the train, the ... employee left the documents on the subway train and they were never recovered." The documents included patients' diagnoses, some of which were HIV/AIDS diagnoses, according to HHS.

Lesson learned: "Anyone who has people who as a part of their function take paper files containing PHI in their cars or to other off-site locations should consider the need to tighten their PHI safeguards," says Dallas attorney

Cynthia Stamer.

"Organizations should have a policy stating that documents with PHI taken offsite should be in a locked container, such as a briefcase," says **Jim Sheldon-Dean,** principal and director of compliance services with Lewis Creek Systems LLC in Charlotte, Vt. The briefcase or container should also include clear identification on the front to allow someone who finds it to return it to the organization, he adds. "And the policy should indicate that staff should not open the containers and remove the files until they are in a physically secure area where the files won't be lost or there won't be anyone able to look over their shoulder."

Of course, "you always have the threat of someone being careless and violating policy," he says. The facility can, however, conduct audits where someone observes whether people taking PHI offsite leave the premises with the files in a locked briefcase or container, Sheldon-Dean advises.

Keep in mind: "Under the breach law," says Sheldon-Dean, "redacting is excluded as a means of de-identifying information. So even if you lost redacted files, you'd still have to report that as a breach."

On the other hand: Lost or stolen files that had been properly de-identified wouldn't be a breach, Sheldon-Dean adds. But you'd have to remove all the identifiers detailed in the privacy rule, as well as other identifiers in the data, he stresses. "Using only initials or reverse initials should be sufficient, so long as it's not easy for someone else to figure out what the initials mean by cross-referencing with publicly available information."

Education a Critical Component

Also provide a "solid training plan to make sure that staff is aware of the policy, its importance, and the consequences of not following it," Sheldon-Dean stresses. And remind staff about the policy periodically, "especially now that this kind of a lapse in physical security has been shown to be something that HHS OCR will want to penalize."

Driving the point home: "One way to get staff to understand what can happen is to share what we call 'the wall of shame,'" which is the government's website that lists the covered entities that had to report a breach, advises **William**

Oravecz, SM, MBA, chief analyst for HITECH Answers, and managing partner of WTO Associates LLC, a healthcare technology and IT solutions company. "You can see what places have been cited and for what." Oravecz says he thinks that if more organizations knew of that website, they might say: "That's the last thing we need to be on." (To review the listing, go to www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.)