

MDS Alert

HIPAA Compliance: Real-World Cases Highlight Escalating Dangers of Privacy Noncompliance

Nurses take the heat for alleged online privacy violations.

Looking for cautionary scenarios to keep everyone on their toes privacywise? Three recent events provide a heads up about the potential for major HIPAA snafus -- and how to prevent similar problems on your watch.

Scenario No. 1: Online Postings Cross the Privacy Line

In June, several hospital nurses found themselves in HIPAA trouble for allegedly posting patient care-related information on Facebook, according to an article in North County Times. The state health department is now investigating the incident, according to other news accounts. While a pending investigation and hearing may exonerate the nurses, the take-home message is clear:

Be careful what you post. And realize that you can't ever expect privacy in cyberspace, says **Jim S heldon-Dean**, principal and director of compliance services for Lewis Creek Systems LLC in Charlotte, Vt.

"Facebook and Twitter, etc., are useful places for professionals to look for advice from peers," says Sheldon-Dean. "But you have to be careful not to communicate private information or post any identifiable pictures," he says.

Play it completely safe: Some attorneys advise against posting any information about patients in online forums whatsoever. "While the nurse may not post any patient identifying information, you can identify the nurse on Facebook [or other social forums]," says attorney **Rebekah Plowman** with Nelson Mullins Riley & Scarborough LLP in Atlanta. "And people in a small community may know the person the nurse is talking about and thus may be able to make the link." That's different, say experts, than using online discussion forums to address hypothetical situations and scenarios that address various clinical challenges, such as combative behavior or drug interactions. "Those discussions should be generic, such as 'how would you handle a patient who does x, y, or z?'" says attorney **Heather Berchem**, with Murtha Cullina in New Haven, Conn.

Scenario No. 2: Have Laptop, Will Travel

Do you or other staff take their laptops to do preadmission reviews or on home visits for rehab therapy, as examples? In a recent case, a hospice had to alert patients after a staff person's laptop was stolen during a home visit, reported the Park Ridge Herald-Advocate. The computer had "security measures in place," but held patient information such as names, addresses, social security numbers, insurance information, medications, treatments, and diagnoses, the involved hospital relayed in a release.

Also: A stolen laptop in Chicago contained about 10,000 names of TennCare recipients and their confidential information, including social security numbers, according to media accounts.

Take away: Any portable device containing PHI (iPhones, iPads, laptops, memory sticks, etc.) should have passwords protection and encrypted data, including text messages, advises Sheldon-Dean. "If it isn't encrypted and you lose the device, that's begging for penalties." And both the individual and the organization can be liable, particularly when they didn't take appropriate security measures, he adds. "New penalties for willful neglect, going into effect in 2011, will include a mandatory minimum penalty of \$10,000. And the penalties can now go into the millions of dollars." The facility should have policies and education to discourage attending physicians from communicating using non-encrypted text messages, advises Berchem. And staff should not text to a cell phone that doesn't have encryption, she adds. "You can transmit unencrypted information that doesn't identify the resident."

For example, you could text that "the resident's X-rays we spoke of two hours ago are negative." You can't, of course, always use that approach because "it can get confusing as to which resident you're talking about," Berchem adds.

Tip: Maintain control at all times of portable devices that contain PHI, advises Plowman. For example, put a cell phone with PHI on it in a holster attached to your person, she suggests.

Scenario N o. 3: Curiosity T rumps Privacy Concerns

In a recent case, a UCLA healthcare researcher received a four-month federal prison sentence for reading hundreds of what were mostly celebrity and high-profile patients' records. Department of Justice investigators did not find any evidence that the employee attempted to use or sell the information. Rather, he apparently sought the information out of curiosity, according to a DOJ release (www.justice.gov/usao/cac/pressroom/pr2010/079.html).

Take-away message: "One could question if the healthcare organization could have done more to prevent that kind of thing by limiting access to records," says Sheldon-Dean. Education is key to make sure caregiving staff know not to look at medical records of patients who aren't under their care, says Plowman. Sometimes healthcare staff will read a chart belonging to someone they know but aren't taking care of out of concern for the person, she observes.

But if a staff person shares that patient's PHI with another person, that person can then tell another person -- and the patient's PHI has been "disclosed to the general public."