Codify
BY AAPC

Health Information Compliance Alert

Privacy: Follow 3 Tips When Handling Patient Privacy Concerns at Your Organization

Hint: Paper files can be breached just as easily as electronic files.

You may be sure that you've dotted all of your i's and crossed all of your t's, but if you miss even a small piece of the privacy puzzle, you can compromise your entire system. Take a look at these three reminders to ensure that yourprivacy program is on track:

1. Don't Let Paper Get Lost in the Shuffle. You may think of patient privacy exclusively in terms of protecting electronic patient data, but paper files are just as likely to be compromised. "With the advent of the HITECH changes, breaches occurring with paper records will be treated the same way as electronic data," says **Gregory Michaels,** manager of security and compliance solutions at **BluePrint Healthcare IT** in Cranbury, N.J.

"Doctors may take paper records home as opposed to USB keys, or they may take paper records in their car with them to the office or hospital, and obviously those things have the same value in terms of the information contained in them," Michaels advises.

Even in facilities where paper records are stored securely, there's still a chance that the information on them might be exposed.

"In some hospitals, the main medical record area is very well secured, but other departments may have access to records, take them from the room, and storethem temporarily while using them, and may not be keeping them secure," he says.

"Even if we can move to 50 or 60 percent of medical practices being fully electronic in the next few years, we're still looking at a long time before paper is eliminated, so make sure any PHI stored on paper in your office is secure."

Even before the HITECH Act came into existence, practices were always advised to handle PHI securely -- whether it was on paper or stored electronically.

"It has been the case for a long time, and it's still the case, that healthcare providers should not throw PHI into the trash," says **Michelle Wilcox DeBarge**, Esq., with **Wiggin and Dana LLP** in Hartford, Conn. "Proper disposal practices should be in place (for instance, shredding)," she says. "And now under HITECH, the breach notification requirements don't just apply to breaches of electronic information -- oral or paper disclosures fall under the Act as well," she advises.

2. Know That Patients Are Aware. You've asked patients to sign a HIPAA privacy form, now they're content, right? Not necessarily. "The HITECH Act imposed an affirmative obligation on the government agency overseeing the HIPAA program to investigate compliance breaches," DeBarge says. "Previously it was driven by complaints only, but they now have an obligation to affirmatively audit and monitor."

Plus: The government has been hiring people to ensure compliance and will be providing education programs to the public, "and we're expecting a lot of awareness, and for patients to be asking more questions about the use of their private health information going forward," says **Peter Courtway,** chief information officer for **Danbury Health Systems** in Connecticut.

"There is also a provision under HITECH that will allow individuals who have been harmed by a breach to have a share in the proceeds of the penalties," DeBarge says. "We don't have the details yet, but this is another reason that patients will have incentive to pay attention."

3. Don't Forget the Front Lines. You may be compromising patient data in other ways besides electronic and paper breaches. Perform a walkthrough in your practice or organization to ensure that no other leaks exist.

For instance: One compliance officer walked through her practice and was pleased to see that computer monitors at the front desk had been turned so that patients in the waiting area could not see the screens. However, upon going to the elevators, she realized that the monitors were viewable through the glass entryway, and that anyone in the building's lobby could see the data.