Part B Insider (Multispecialty) Coding Alert

Patient Privacy: This is the Single Biggest Source of HIPAA Breaches

Hint: Most breaches are due to passive errors, not deliberate disclosures.

Based on evidence from recent HIPAA investigations, it's not what you're doing that will likely subject you to a breach enforcement—it's what you're **not** doing that could land you in hot water.

That was the word from **Jim Sheldon-Dean,** director of compliance services with Lewis Creek Systems, LLC, during the June 30 Audioeducator.com webinar "HIPAA Audits in 2015—Being Prepared and Avoiding Penalties."

The single biggest source of HIPAA breaches for both small and big breaches was theft, he said, which means that your failure to secure portable devices, cloud-based data, email passwords and other PHI-heavy sources is what's putting you at the biggest risk.

Previous Data Shows You the Way

During previous reports to Congress in 2009 and 2010 about breaches impacting 500 or more individuals' protected health information (PHI), 15 percent of breaches were due to loss, 56 percent to theft and another five percent blamed on improper disposal. These all represent old-fashioned physical security of valuable data, which means that "if you'd just kept your hands on it, whether it's paper or electronic, you wouldn't have had a problem," Sheldon-Dean said.

Another 17 percent of significant breaches in this category were caused by unauthorized access or disclosure, and six percent by hacking.

For smaller breaches affecting fewer than 500 individuals, 53 percent of the breaches were due to theft and another 18 percent were due to unauthorized access or disclosure.

The takeaway: Make sure your data is all encrypted and secured, especially on portable items such as laptops, smartphones and memory sticks, which can easily be lost.

You should also have clear and well-documented safeguards on the portable media that handle ePHI, reduce risk via enterprise storage, check fax numbers and addresses regularly, be careful handling PHI that's mailed and raise the security awareness of your staff members, Sheldon-Dean added.

Know What Constitutes a Breach

Before you can start identifying potential breaches at your practice, it's important to know what the law says. "According to the Privacy Rule, a breach is any acquisition, access, use or disclosure in violation in the privacy rule—and that covers a lot," Sheldon-Dean says. However, there are exceptions under which you aren't required to report the breach, including the following, he adds:

- **If the data is destroyed or secured according to HHS guidance.** "Make sure you use good quality, secure encryption," he said.
- **Unintentional internal use, in good faith.** For instance, if you put a folder on the wrong desk and a physician opens it, says, "Oh, these aren't my patient's notes, these belong to someone else" and closes it, you aren't required to report that.
- **Inadvertent internal use, within job scope.** For example, someone looks up the records for Mary Smith but opens the notes for the wrong Mary Smith, realizes her mistake, and then closes out the notes.

- **Information cannot be retained.** For instance, you lose a box of medical records and you find them the next day with the box still sealed the way you left them, and you know the information was not breached.

If you don't meet these exceptions but you can prove there was a low probability of compromise based on your risk assessment, you may still be in the clear, Sheldon-Dean said. The risk assessment must include a detailing of what information was in the records, how well identified the PHI was, and whether its release would be "adverse to the individual." You'll also have to assess to whom it was disclosed, whether it was actually acquired or viewed and the extent of mitigation.

For instance: Suppose you fax an allergy test result with just patient initials to the wrong physician. The physician calls you and says, "You meant to send this to someone else, we're shredding it." That's a low probability of compromise, with very little identifying patient information on it, Sheldon-Dean says.

Perform Your Risk Analysis

Whenever you do a risk analysis, remember that each risk issue has an impact and a likelihood, he noted. The impact refers to how great the damage would be a lot of information about a lot of people with excessive detail would have a greater impact. Likelihood refers to how likely it is that the risk issue would become a reality.

Once you analyze your practice's risk, if you find breaches to report, don't just tell the government, "We had a breach." Instead, say, "We had a breach, we know what happened, we fixed the problem, we've had some improved training, policies and procedures, we've done some auditing to make sure everything is better, and you'll never hear about this problem from us ever again." If you include that type of information with your report, they'll be less likely to ask further questions, Sheldon-Dean advised.

Audits Are Coming

There have been some indications about the upcoming HIPAA audit program and the fact that the government is actually going through the selection process for the audit targets, but there has not yet been a formal discussion outlining the details, Sheldon-Dean said. A description of when the audit program will hit and how it will work hasn't been issued yet, but "we do know it's getting closer and closer and they are hiring people to run the program...so they're getting there," he added.

You could be the subject of an audit after reporting your own breach, being the target of a complaint or via random audit, he said. If you do get audited, show the auditors that you have policies and procedures in place as required by the HIPAA Privacy, Security and Breach Notification Rules, and demonstrate that you've been using them. For example, show your training materials and rosters, show your security incident reports, and other supporting documentation.

Secure Your Texts, Emails

One of the enforcement actions that the OCR previously announced involved a cardiac surgery practice in Phoenix that was fined $100,000 because their doctors were using plain Gmail and plain Google calendar for their professional communications involving protected health information. The emails and calendars were not encrypted and were easy for others to access, creating a violation. Therefore, you should ensure that your email systems and calendars are well secured.

Likewise, texting is not secure unless both parties use a secure texting app, but if they aren't using secure technology and are exchanging PHI, they could be in violation of the rules, Sheldon-Dean added. "Plain texting involving PHI is a very insidious problem and is probably the biggest problem that has snuck in the back door because people start using it and they see how easy it is."