Part B Insider (Multispecialty) Coding Alert

Patient Privacy: HIPAA Audits Begin in Two Months--Are You Ready?

Oct. 1, 2013 is the planned start date for the OCR to start auditing medical practices for HIPAA compliance.

You may have heard inklings of other Part B practices undergoing HIPAA audits, but because the scope of the audits was so small, you didn't prepare for one yourself. That's all about to change, as the Office of Civil Rights' (OCR's) pilot HIPAA audit comes to a close, and the permanent audits begin in October. You can prepare now for the audits that could be coming your way using a few simple tips that **Jim Sheldon-Dean**, director of compliance services at Lewis Creek Systems, shared during a June Coding Institute audioconference entitled "The HIPAA Audit Protocol Documenting Compliance Before You Get an Audit Notice."

You Can't Wait Until 2014

If you heard that HIPAA audits don't begin until 2014, you're both correct and incorrect. "They say the new audit program is beginning in 2014," Sheldon-Dean says. "But of course what they're talking about is the federal fiscal year 2014, which begins on Oct. 1, 2013."

Keep in mind, however, that auditors aren't trying to fill a quota of nailing practices on broken privacy laws. "Enforcement is not the point of the audits," Sheldon-Dean says. "The point of the audits is to review compliance and find problems. But if they see a problem that may be worth some kind of enforcement action, they're not averse to discussing that with those who would be going in to levy the fines."

The penalty that you may not be familiar with, because it's new, is the penalty called "Willful Neglect," Sheldon-Dean says. "It means if you have not been paying attention, if you have not been doing what you should be doing for compliance and there's some kind of problem, they can levy some significant fines. It gets very expensive very quickly, so you want to make sure you don't ignore the rules."

Because the Willful Neglect penalties are only assessed if your practice didn't implement HIPAA into your practice and continue to follow up on ensuring your compliance with them, practices who have a HIPAA breach despite their best effort in maintaining privacy and security shouldn't be affected by it.

Consider Risk Assessment

To confirm that your practice is operating effectively under the HIPAA guidelines, you should perform a risk assessment, Sheldon-Dean suggests. You don't need to perform one more than every year unless you're installing new systems, hiring new business associates, or making any other significant changes that could alter your privacy and security compliance.

Keep in mind: Practices that get meaningful use funding should be committed to performing risk assessments annually, Sheldon-Dean says. "If you're getting federal money for your electronic health record, it does need to be updated on an annual basis."

Although the government does not offer a risk assessment tool per se, the National Institute of Standards and Technology does publish risk assessment guidelines in its document "An Introductory Resource Guide for Implementing

the HIPAA Security Rule." The document guides you in how to identify realistic threats to protected health information (PHI) in your office as well as potential vulnerabilities. You'll then weigh those against your current security controls to determine your actual risk level. You can access the document at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

Who Counts As 'Business Associates?'

As most practices are aware, one of the main changes that the HIPAA program updated during its HITECH Final Rule (which takes effect Sept. 23) is that business associates are more accountable than ever under HIPAA. Both business associates and their subcontractors will have to maintain PHI just as your practice would. Your business associates typically include entities such as your billing service, your offsite coding contractors, or your contracted in-house laboratory, for instance.

But how broad is the "business associate" label? Does it expand to your office's cleaning service? "Business associate agreements include organizations that may create, receive, maintain or transmit health information," Sheldon-Dean says. Since your cleaning staff is not accessing health information in any way, they won't typically be considered "business associates."

"The cleaning staff should be under a confidentiality agreement but not necessarily a business associate agreement," Sheldon-Dean advises. "If you start asking your cleaning staff to look in the waste baskets and bring you any pieces of paper that have health information as kind of a compliance check, then they are doing something with PHI on your half and they'd be a business associate."

Use HHS Guidance to Prepare

If you want to ensure that you could pass a HIPAA audit, check out the HIPAA Audit Protocol, which includes 169 questions and quite a few sub-questions. This can help you determine the type of documentation you might be asked to submit if you're ever subject to a HIPAA audit. The document is available at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.