Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

Patient Privacy: It's Official: HIPAA Audits Are in Full Swing

Here's how you can be ready in case an audit comes your way.

You've been hearing for years that HIPAA audits are around the bend, but with the Office of Civil Rights (OCR) repeatedly delaying them, many practices were beginning to wonder if the privacy audits were simply an urban myth. An OCR announcement last week, however, confirmed that phase two audits are very realand are already in motion.

What is phase two? During phase one of the HIPAA audits, the OCR implemented a pilot program to essentially establish the audit protocol. Now that phase two has started, OCR has pledged to audit not only covered entities, but also their business associates. Although most of the audits will be "desk audits," some will be on-site audits, the OCR said in its announcement.

New Audits Are Extension of Phase One

Fortunately, practices familiar with the phase one audits won't find the phase two process that much different, says attorney **Neil Eggeson** of Eggeson Appellate Services in Indianapolis. "The phase one audits involved a three-step process: After creating the audit protocols (step one), OCR conducted an initial wave of 20 audits to test the protocols (step two). After revising the protocols, OCR conducted the rest of its audits," he says. The total number of audits involved during phase one included only 115 covered entities.

"The phase two audit protocol is essentially a further revision of the phase one protocol streamlined to focus on specific areas," Eggeson says. Due to that fact, OCR does not foresee revising the audit protocols further. "The first round of desk audits will focus on covered entities, the second round of desk audits will focus on business associates, and the third round of on-site audits will be drawn from those entities audited during the first two rounds. As all desk audits are expected to be completed by December 2016, it would seem that phase two is going to be limited to roughly 200 entities total (including health plans and clearinghouses)."

Don't Stress Over 'Business Associate' Links

Some practices are concerned that if their business associates (BAs) fail an audit, the BA will drag the practice down with it. Fortunately, however, that doesn't appear to be a big risk.

"Strictly speaking, under HITECH a covered entity is not responsible for its business associate's compliance," Eggeson tells Part B Insider. "Thus, if a business associate fails a Phase two audit, it should not affect the covered entity's own audit performance."

If, however, you know about a BA's privacy issues prior to an audit, then you do bear some responsibility to address it. "If a medical practice becomes aware of a deficiency in its business associate's compliance with the Privacy Rule, the medical practice must take steps to correct or mitigate that risk," Eggeson says. "Consequently, medical practices are well within their rights to demand broader assurances from their business associates including a periodic review/audit of their business associates' compliance."

Assuming your practice is already familiar with your business associates' privacy practices and you believe that they are in compliance with HIPAA, then you shouldn't have to "pre-audit" them to make sure they are on the straight and narrow.

Prepare Now for Audits

During the OCR's desk audits, the agency will be reviewing privacy policies relating to the Privacy, Security, and Breach Notification Rules, says San Francisco-based privacy attorney **Diana Maier**. "OCR has also said that they expect audited entities to respond to their initial request for documentation within ten business days by submitting documents electronically via their secure, online portal. To prepare for a potential audit, I always recommend that covered entities and business associates ensure that they have written privacy policies consistent with their requirements under HIPAA."

In addition, she recommends that her clients run the Security Risk Assessment Tool, which is available online. "This isn't required by the HIPAA Security Rule, but it is meant to assist with a risk assessment and can be a great resource for identifying areas of vulnerability," she advises. Maier also suggests the following steps during your audit preparation:

- If a covered entity is required to provide a notice of their privacy policy, they should make sure they have this policy in place and are distributing it appropriately.
- Business associates should review their agreements with covered entities to make sure they are doing what they said they would do.
- Another critical part is that covered entities and business associates should make sure they understand those policies and are following them. If they do this, they are far more likely to get through an audit without any major issues.

Be Ready to Prove You Have an Ongoing Compliance Program

During the phase one audits, the OCR found that one of the biggest deficiencies among practices was in the area of risk assessment, Eggeson says. "Because of that, medical practices should be conducting regular security risk assessments and should be able to document the steps taken to correct security risks. Similarly, the medical practice should be able to document an ongoing, comprehensive HIPAA compliance program (including periodic reviews and updates of that program)."

Although it's never too late to tighten up your HIPAA program, chances are that if you get an audit notification today and you haven't yet launched a privacy program, you could get zinged by an auditor. "If a medical practice has not taken these steps by now, it likely is too late for the practice to generate the necessary paper trail prior to a phase two audit," Eggeson says.

In addition to the risk assessments and HIPAA compliance program, practices should generate an inventory of all business associates, he adds. "All audited providers will be expected to produce a list of its business associates, so having that list ready will be helpful in preparing for a phase two audit, Eggeson advises.

"Moreover, practices should review all policies related to security, breach notification, and protected health information to ensure that they are up-to-date AND take into account all technologies used by the practice (eg, cloud storage). In addition, the practice should have a breach notification policy that accurately tracks the requirements found in the Breach Notification Standards, and it should have a compliant Notice of Privacy Practices."

Resource: To read more about Phase two of the HIPAA audits, visit http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.