Codify
BY AAPC

Health Information Compliance Alert

Audits: Phase 2 HIPAA Audits Are Beginning -- Here's How To Survive Them

Focus on these areas to prepare for new round of audits.

If you're one of the "lucky" few selected for a Phase 2 audit, you'd better hurry up and get ready. On March 21, the **HHS Office for Civil Rights** (OCR) announced the official launch of the Phase 2 HIPAA audit program and the findings of these audits could have real consequences.

Phase 1 Results Dictate Phase 2 Protocols

In the Phase 1 HIPAA audits, OCR used a three-step process involving creating the audit protocols, conducting an initial wave of 20 audits to test the protocols, and revising the protocols and conducting the rest of the audits, notes attorney **Neal F. Eggeson, JD** of **Eggeson Appellate Services** in Indianapolis. Phase 1 involved only 115 covered entities (CEs).

"The Phase 2 audit protocol is essentially a further revision of the Phase 1 protocol, streamlined to focus on specific areas," Eggeson explains. "Because of this, OCR does not anticipate revising its audit protocols further."

The first round of audits will be desk audits and focus on CEs, while the second round of desk audits will focus on business associates (BAs). The third round will be on-site audits, and OCR will draw the selected entities for these on-site audits from those that participated in the first two rounds.

Timeline: "As all desk audits are expected to be completed by December 2016, it would seem that Phase 2 is going to be limited to roughly 200 entities TOTAL (including health plans and clearinghouses)," Eggeson notes.

Don't Let OCR's Email Go Astray

OCR is beginning the audit process by sending emails out to CEs and BAs requesting contact information. Then, OCR will send you a pre-audit questionnaire to gather data about potential auditees' size, type, and operations. OCR will use this data along with other information to create potential audit subject pools.

Watch out: If you don't respond to the OCR's email, you're not off the hook. OCR said it will "use publicly available information about the entity to create its audit subject pool." So even if you don't respond, OCR may still select you for an audit or you may be subject to a compliance review.

Also, beware that your email system may incorrectly flag OCR's email as spam, so make sure you check your junk or spam email folder for emails from OCR especially if your spam filtering and virus protection are automatically enabled.

Post-audit: After OCR provides its draft findings, audited entities will then have 10 business days to review the findings and provide written comments, noted attorneys **Carolyn Metnick** and **Elizabeth Hodge** of **Akerman LLP** in a March 22 blog posting. Afterward, the auditor will prepare a final report within 30 business days following receipt of the entity's response.

Prepare Now: What You Need to Do

"One of the largest deficiencies discovered during the Phase 1 audits 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."

You can use the Security Risk Assessment Tool (www.healthit.gov/providers-professionals/security-risk-assessment-tool), provided by HHS. "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," suggests attorney **Diana Maier** of the **Law Offices of Diana Maier** in San Francisco.

Beware: Similarly, you should be able to document an ongoing, comprehensive HIPAA compliance program, including periodic reviews and updates of that program, Eggeson instructs. "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 2 audit."

Nevertheless, "it's never too late to tighten up your privacy practices," Maier notes. And in the desk audits, OCR will review your privacy policies relating to the Privacy, Security, and Breach Notification Rules. But OCR has also said that it expects audited entities to respond to its initial request for documentation within 10 business days by submitting documents electronically via its secure online portal.

Get Your Documents in Order

In addition to the risk assessments and HIPAA compliance program, you should generate an inventory of all your BAs, Eggeson says. OCR will expect all audited providers to produce a list of its BAs, "so having that list ready will be helpful in preparing for a Phase 2 audit."

"Moreover, practices should review all policies related to security, breach notification, and protected health information [PHI] to ensure that they are up-to-date AND take into account all technologies used by the practice (e.g., cloud storage)," Eggeson adds. "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."

What's more: Another critical part of preparing for the Phase 2 audits is for both CEs and BAs to make sure they understand their BA agreements (BAAs) and their HIPAA policies, and that they are following those policies, Maier stresses. "If they do this, they are far more likely to get through an audit without any major issues."

Keep Your Eyes Peeled for New Procedures

OCR also said it will post updated audit protocols on its website closer to conducting the 2016 audits. OCR will update the protocols to reflect the HIPAA Omnibus Final Rule. You can use the updated protocol as a tool to conduct your own internal self-audit as part of your HIPAA compliance activities, according to OCR.

Resources: For more information on the HIPAA audit program, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html. To read OCR's announcement, visit www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html. And you can view the audit pre-screening questionnaire at www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html.