What to Expect When Phase 2 HIPAA Audits Begin

Save to myBoK

By Angela Rose, MHA, RHIA, CHPS, FAHIMA

The HITECH Omnibus Rule mandated that the US Department of Health and Human Services (HHS) conduct periodic audits on the privacy and security compliance of covered entities and business associates. It was during the Office for Civil Rights (OCR) update session on March 21, 2016 at the 2016 HIPAA Summit in Washington, DC, that Deven McGraw, OCR's deputy director of health information privacy, announced that "Phase 2" of the HIPAA audits had officially begun.

The first HIPAA audit was actually conducted by the Office of the Inspector General (OIG) in 2008 as a result of the OIG's review of the Centers for Medicare and Medicaid Services' (CMS) oversight efforts.[1] CMS was the oversight agency for the HIPAA Security Rule until 2009. The second and third rounds of audits were conducted under CMS' authority through PricewaterhouseCoopers[2] in 2008 and Quality Software Services[3] in 2009, respectively. Phase 1, or round four, of the HIPAA audits was conducted in 2012 and included 115 covered entities of all types and sizes.

This upcoming round of audits is referred to as "Phase 2," but it is actually the fifth round of audits to be conducted to determine overall HIPAA privacy and security compliance in the industry. Phase 2 will include business associates as well for the first time. OCR is expected to conduct 200 desk and onsite audits to complete Phase 2, with onsite audits expected to begin later this year. It was stated that an entity receiving a desk audit may be subject to an onsite audit if deemed appropriate by OCR.

Audit Selection and Notification

Covered entities and business associates will be selected for audits based on size, type, affiliations, whether public or private, and geographic factors. Covered entities and business associates that are chosen for a possible audit will be sent a contact information and address verification e-mail. A timely response to OCR is expected, and a pre-audit questionnaire will follow. The questionnaire will provide information for OCR to build their pool of potential auditees. Even if a potential auditee does not respond, they may still be selected for an audit. Covered entities are also encouraged to ensure their list of business associates is both current and readily available.

Upon selection for an audit, OCR will send a formal letter via e-mail to the confirmed contact with the details of the audit as well as an introduction to the audit team.

Desk Audits

One of the initial requests from OCR will be the submission of documentation through their secure portal. OCR expects auditees to complete this within 10 business days of the request.[4] Desk audits will primarily focus on the review of policies and procedures adopted by the selected covered entities and business associates. OCR will notify and request documentation from selected business associates during the desk audit of a covered entity.

Draft findings will be provided to the covered entity upon completion of the desk audit. The covered entity will have 10 business days to respond with any comments. A final report from the auditor will be provided to the covered entity and any selected business associates 30 business days from the auditee's response. All desk audits are expected to be completed by the end of 2016.

On-site Audits

Those selected for an on-site audit will also be notified via e-mail. An entrance conference will be scheduled to explain the details of the on-site audit process. On-site audits are estimated to last three to five days depending upon the size of the entity.

On-site audits take a deeper dive looking at a broader spectrum of the HIPAA requirements than the desk audits. They are intended to be more inclusive and hands on. Similar to the desk audits, a report of the findings will be issued allowing 10 business days for an auditee to comment. A final report will be issued 30 days from the receipt date of any comments.

Audit Findings

The intended use of the findings from the Phase 2 audits is to help OCR determine what type of guidance and tools would be most useful to the industry. The findings will help OCR get a better grasp on compliance within the industry and identify gaps where help is needed most. OCR does not intend to post any individual audit results or a list of audited entities.

Whether an entity is notified of an audit or not, at a minimum workforce members should be properly trained on the following items, which should be regularly reviewed and updated:

- Security risk analysis
- Breach policy and procedures
- Privacy policy and procedures
- Security policy and procedures

Notes

[1] Letter from Department of Health and Human Services' Inspector General Daniel R. Levinson to Centers for Medicare and Medicaid Services Acting Administrator Kerry Weems, October 27, 2008. http://oig.hhs.gov/oas/reports/region4/40705064.pdf.

[2] Dinh, Angela K. "Teeth for HIPAA in 2008? CMS Announces Plans for Security 'Assessments.'" *Journal of AHIMA* 79, no. 3 (March 2008): 62-63.

[3] Dinh, Angela K. "CMS's 2009 Security Assessment Process." *Journal of AHIMA* 80, no. 9 (September 2009): 50-51.

[4] US Department of Health and Human Services. "HIPAA Privacy, Security, and Breach Notification Audit Program." www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#timeline.

Angela Rose (angela.rose@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Rose, Angela Dinh. "What to Expect When Phase 2 HIPAA Audits Begin" *Journal of AHIMA* 87, no.6 (June 2016): 34-35.