Industry Awaits Phase 2 of HIPAA Audit Program

By Don Asmonga

The wait for the second round of mandated privacy and security audits from the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) continues. OCR is currently working through final details for the revised audit plan as they await finalization of new technology that will enable those being audited the ability to submit information electronically.

The HIPAA audit program began with the passage of regulations required in the Health Information Technology for Economic and Clinical Health Act (HITECH) that was included in the $787 billion American Recovery and Reinvestment Act (ARRA) in February 2009. The ARRA-HITECH language required HHS to conduct "periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification Standards."

To do this, OCR looked to do the following:[1]

1. Seek a comprehensive, flexible process for analyzing entity efforts to provide regulatory protections and individual rights
2. Identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools
3. Encourage consistent attention to compliance activities

Results of Phase 1 Audits

The OCR audit program commenced with a pilot from 2011 to 2012 that included 115 performance audits—the first 20 to test the original protocol and the next 95 using a modified protocol.[2] Health plans, clearinghouses, and providers were audited.

The primary focus areas for the audits included 11 modules:

- Breach notification
- Security: Administrative safeguards, physical safeguards, and technical safeguards
- Privacy: Notice of Privacy Practices, rights to request privacy protection of personal health information (PHI), access of individuals to PHI, administrative requirements, uses and disclosures of PHI, amendment of PHI, and accounting of disclosures

According to OCR, initial overall audit findings and observations (or terms that indicate a violation was committed) using the modules above revealed there were no findings or observations for 13 entities (11 percent). This included two providers, nine health plans, and two clearinghouses. Security accounted for 60 percent of the findings and observations, only 28 percent of the total. Also, providers had a greater proportion of findings and observations (65 percent) than reflected by their proportion of the total set (53 percent). Smaller entities were shown to struggle with all three areas, having issues in breach notification, security, and privacy.

The results from the security portion of the audits showed that:

- Of the 59 providers audited, 58 had at least one security finding or observation
- There were no complete and accurate risk assessments in two-thirds of the entities audited, which included 47 of 59 providers, 20 out of 35 health plans, and two out of seven clearinghouses
- As for security addressable implementation specifications, most entities without a finding or observation met the standard by fully implementing the addressable specification

The most common overall finding of the audits was that the entity was unaware of the security requirements.

Phase 2 Waiting on Technology Upgrades

As OCR continues to mull the results from Phase 1, they wait in earnest to move forward with Phase 2, which will enable OCR to audit any covered entity and any business associate.

During a September 2014 presentation at the Healthcare Information and Management Systems Society (HIMSS) Security Forum, Linda Sanches, senior advisor for health information privacy at OCR, stated that the agency will begin the audits by sending pre-screening surveys to covered entities and then their business associates. In the process, OCR will ask the covered entities to identify their business associates and provide the business associate's contact information. OCR will randomly select covered entity and business associate audit subjects for 2015 from the information received and a National Provider Index. Those selected will be a mix of covered entities from across the country. OCR will then proceed with desk audits and, as resources permit, comprehensive onsite audits.

A panel discussion during this year's AHIMA convention titled "Health Information Privacy: Privacy, Security, Breach Notification Rules and Enforcement" included three OCR staff members who confirmed that the covered entities and business associates for the Phase 2 audits had been selected but not yet notified.

Once underway, Phase 2 of the audit process will first train its focus on covered entities and look at their risk analysis and risk management areas of security, the content and timeliness of their breach notifications, and their Notice of Privacy Practices, mandated by the HIPAA Privacy and Security Rules. Following that effort, the focus will shift to business associates and their risk analysis and risk management security protocols and whether or not the business associates are complying with breach reporting requirements they must make to their partnered covered entity.

Attention will then return to the covered entities, and auditors will look at additional security requirements that include device and media controls and transmission security. In addition, OCR will review the covered entity's ability to meet the privacy requirements related to safeguard policies and procedures and training. Finally, the focus will include encryption and decryption, facility access controls (physical), and other areas of high risk as identified by the 2012 Phase 1 audits, breach reports, and complaints.

As mentioned, one of the primary reasons for the delay in the audit program was the development of technology to enable the better collection and processing of audit data. The original plan from OCR was to conduct 400 desk audits of both covered entities and business associates. With an influx of some additional funding, OCR has reduced the number of desk audits to approximately 200 to enable more live, onsite audits of covered entities and business associates. Whether a desk audit or a live audit is conducted, it will be important to ensure that an organizations' documentation is stellar and includes formal policies and procedures for risk mitigation, sanctions process, and the documentation of sanctions and incidents.

Being prepared for an audit comes with completing a regular internal risk analysis. As noted earlier in the security audit results from Phase 1, nearly two-thirds of those audited did not complete a comprehensive risk assessment. This will certainly be an area of focus in Phase 2. Regular risk analyses can assist with identifying gaps that may have arisen through changes and updates in processes, technology, or even staff. Without doing this, a covered entity could put themselves in jeopardy for some hefty fines that range into the millions of dollars.

Prepare Now for Next Audit Round

Sometimes waiting is the hardest part. As of press time in early December, OCR was expected to announce the details and timeline for the Phase 2 audits in the coming weeks or months. If an organization hasn't started already, it is important to review available, excellent resources provided by AHIMA, read information on the OCR website, and talk with in-house HIPAA experts to not only ensure that privacy, security, and breach procedures are up-to-date and air tight, but that the organization is also prepared for a potential audit.

More information on the documentation needed for the audit can be found at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html, and on the OCR Audit Program Protocol website at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html. There are also helpful resources in AHIMA's Engage communities. Some HIM and HIPAA privacy and security consulting companies also provide mock audit services to prepare organizations for OCR audits.

Notes

[1] Sanches, Linda. "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2." Presented at the HCCA Compliance Institute, March 31, 2014.

[2] Ibid.

Don Asmonga (dasmonga@privacyanalytics.ca) is vice president, standards and government affairs, at Privacy Analytics.
