CMS's 2009 Security Assessment Process

by **Angela K. Dinh**, MHA, RHIA

In 2008 the Centers for Medicare and Medicaid Services (CMS) conducted 10 HIPAA security assessments in covered entities (CEs) nationwide. CMS's stated purpose was not to identify flaws but to gain a true understanding of industry compliance with the HIPAA security rule.

CMS contracted PriceWaterhouseCoopers to carry out and complete all assessments, which were selected on a complaint-driven basis. In other words, the sites were chosen from a pool of CEs that already had complaints filed against them.

In May 2009 CMS and the National Institute of Standards and Technology (NIST) held a two-day conference focusing on the security rule and safeguarding protected health information. This article reviews the conference highlights regarding CMS's security assessments.

What Happened in 2008?

As noted, the assessments conducted in 2008 were chosen from a pool of existing complaints. According to Elizabeth Holland from the Office of E-Health Standards and Services (OESS) under CMS, the most common complaints involved access management, access control, security awareness and training, incident procedures, and device and media controls.

Covered entities that were assessed by PriceWaterhouseCoopers included nine providers (consisting of seven hospitals, one home care/hospice provider, and one pharmacy) and one health plan. The assessments revealed issues with lack of training, inadequate physical security, remote access, and business associate agreements.

CMS also identified some of the main struggles, including proper and current risk assessments, up-to-date policies and procedures, appropriate training or retraining, work force clearance, encryption, and workstation security. A complete analysis and summary of the 2008 findings is available on the CMS Web site.[1]

CMS's 2009 Plan

CMS announced major changes to the program for 2009. The first involves who will actually be carrying out the assessments. CMS has contracted with a new vendor, Quality Software Services (QSSI), to complete six assessments throughout 2009.

Another shift in CMS's method is in how CEs are selected for assessment. In 2009 they were chosen based on type and geographic location.

The 2009 assessments are taking place in Florida, California, New York, Illinois, Minnesota, and Washington. The six covered entities selected include three health plans, one clearinghouse, and two providers (a skilled nursing facility and a federally qualified health center).

Outlining the Assessment Process

The assessment process will include the following steps, as identified at the CMS and NIST conference:

1. A CE is randomly selected based on type and geographic location.
2. A letter is sent to the CE via certified mail. The letter includes proposed review dates; a proposed date for pre-entrance call to include CMS, QSSI, and the CE; and a request for working space with electric, phone, and Internet connections.
3. Documents, policies, and procedures under review will be requested from the CE in a list format known as the provided by client, or PBC, list. A sample list of types of documents that can be requested can be found on the CMS Web site.[2]

4. The CE sends the requested documents, policies, and procedures on a "flow basis" for review. This differs from 2008 in that last year's reviewers just walked into the CE for review.
5. Documents, policies, and procedures are assessed for compliance with HIPAA regulations.
6. Periodic (weekly or biweekly) pre-review (prior to on-site visit) conference calls will be set up with the CE.
7. Questions are formulated based on review of documents, policies, and procedures.
8. Reviewers arrive on site for five business days or fewer. They will conduct staff interviews. CEs will be notified which staff members will be interviewed prior to the interviews; however, access to all employees is requested. CMS published a list of likely candidates to be interviewed on its Web site, which includes senior leadership, the compliance officer, and the director of training.[3] Any additional documents not sent prior to the on-site review will be completed. Technical controls will be reviewed. Any past review and audits completed also will be reviewed.
9. A draft report is submitted to the CE.
10. The CE reviews and submits comments back to CMS, which makes changes as needed.
11. A final report of findings is filed. A corrective action plan is issued, if needed.

Advice from CMS

During an educational session at the conference, Michael Mellor, a security official from CMS's Office of Information Services, offered simple advice to entities preparing for a review. First, he advised entities to embrace the review and remind staff that the reviewers are there to help, not to scrutinize. He also recommended that the institution be organized and compile all the necessary information before the reviewer arrives on-site.

Mellor advised entities to tell the truth, be accurate, and always keep lines of communication open. "Pick your battles. It's great to question [the reviewers]," Mellor said, "but be choosy. Don't make it difficult."

Finally, Mellor noted that reviewers will "look at old audits, and if there is the same deficiency, that's a problem."

Be Proactive

The most important step for entities that are chosen for a security assessment is to be proactive. CEs should review all policies and procedures related to security compliance for relevance and test staff against those policies and procedures for compliance. They should perform an updated risk assessment if one is needed and stay up to date with industry happenings. CMS offers pertinent information and tools online at www.cms.hhs.gov/Enforcement.

HIM professionals are responsible for safeguarding protected health information, and it is essential that they are a part of the team that ensures that protection. By participating in a security assessment, HIM professionals must do what they do best.

Notes

1. Centers for Medicare and Medicaid Services. "HIPAA Compliance Review Analysis and Summary Results." Available online at www.cms.hhs.gov/Enforcement/Downloads/HIPAAComplianceReviewSumtopost508.pdf.
2. Centers for Medicare and Medicaid Services. "Sample—Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews." Available online at www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf.
3. Ibid.

Angela K. Dinh (angela.dinh@ahima.org) is a practice resource manager at AHIMA.

In late July authority for enforcing the security rule transferred to the Office for Civil Rights. What will change? Read the latest at http://journal.ahima.org.

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