Teeth for HIPAA in 2008? CMS Announces Plans for Security "Assessments"

by Angela K. Dinh, MHA, RHIA

Although the HIPAA security rule went into effect in April 2005, the first security audit of a facility's compliance with the HIPAA security rule did not take place until just last year. That audit was heard around the country, awakening every network, firewall, and security plan in existence.

The audit, conducted by the Office of Inspector General (OIG), left everyone wondering what was to be expected in the near future. This anticipation heightened when in January the Centers for Medicare and Medicaid Services (CMS) announced plans for HIPAA assessments in 2008. CMS did not offer many details at the time of the announcement, but it did outline its intended audit process. Here is what was known at press time.

CMS's HIPAA Assessments

This year, CMS plans to take on its enforcement responsibility by conducting HIPAA assessments in 10 to 20 entities nationwide. CMS has contracted with PriceWaterhouseCoopers to conduct the assessments on its behalf. Entities will be selected on a complaint-driven basis; that is, from among those organizations that already have a complaint filed against them.

The results of the assessments will be published and made available as lessons learned in data security. However, facility names will not be disclosed. It is important to note that the OIG audits should not be mistaken with or linked to the CMS HIPAA assessments. OIG selects the entities it audits based on its own criteria, and its audits are driven by its mission, not existing complaints.

In January CMS and the National Institute of Standards and Technology hosted a one-day workshop focusing on HIPAA security implementation and assurance. The director for the Office of E-Health Standards and Services (OESS) emphasized that the assessments will focus on remote access of electronic protected health information. CMS previously published guidance in 2006 regarding remote access, which organizations should find helpful in preparing for an assessment (see the sidebar below).

"The purpose of the assessments is not to identify flaws, but rather gain a true understanding of security in the industry," said Lorraine Doo, a speaker and senior policy advisor for OESS. Doo also provided an outline of the assessment process, which CMS will post on its Web site along with a checklist to assist entities in preparing for an assessment.

Who Enforces What?

Title II, the administrative simplification portion of the HIPAA regulations, includes five sections: transactions, identifiers, security, privacy, and enforcement. The final installment of title II was the enforcement rule, which went into effect March 16, 2006.[1]

The enforcement rule gave authority for the governing and enforcement of the privacy rule to the Office for Civil Rights. It delegated the enforcement of the rest of the HIPAA standards, including the security rule, to CMS.

Note

1. Department of Health and Human Services, Office of the Secretary. "HIPAA Administrative Simplification: Enforcement; Final Rule." 45 CFR Parts 160 and 164. Available online at www.hhs.gov/ocr/hipaa/FinalEnforcementRule06.pdf.

The assessment process will include the following steps as described at the workshop (the process is subject to change):

1. CMS will look at complaints that are primarily security driven (many have a privacy edge).
2. A security level will be assigned to each as designated by CMS.
3. The facility will receive a letter requesting to speak with key staff (e.g., compliance officer, security officer).
4. The interview will be scheduled.
5. The facility will receive a request for information (e.g., records, policies, etc.).
6. The first meeting will be conducted on-site and will last about one week. This will include meetings with staff identified in the letter. The entity may be asked for its risk assessment plan, risk analysis, and other documentation.
7. During a second meeting, CMS will address any items that are outstanding. It will perform a gap analysis, and entities will have a chance to provide anything that was missing earlier.
8. During the final meeting, CMS will assess penalties based on the findings.

How to Prepare for an Audit

CMS's announcement will cause the greatest immediate reaction in facilities with complaints filed against them. All organizations, however, can use the announcement as a strong reminder to monitor and assess their security practices routinely. No one should wait for CMS to come knocking at their facility's door; all organizations should stay current with what is happening in the industry.

Through its Web site, CMS offers tools such as security guidance documents and checklists to assist organizations in preparations and help them validate their compliance levels. Materials are available at www.cms.hhs.gov/securitystandard. At the January meeting, CMS said it will post an outline of the overall assessment process on the site.

The time to assess organizational readiness for an audit is now. Security compliance enforcement is real, and it is happening. The expertise of the HIM professional as part of the security team will help ensure that an organization's compliance is met and maintained.

CMS Guidance on Remote Access

CMS offers guidance on securing electronic protected health information that is accessed or used outside of the organization's four walls. This covers portable media and devices such as USB flash drives, laptops, PDAs, public workstations, wireless access points, and home computers.

"HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information" is available online through the CMS Web site at www.cms.hhs.gov/securitystandard.

CMS offers links to other HIPAA security resources at the same address, including general information and a security educational paper series.

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

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