HIPAA Audits Are Coming: Are You Prepared?

By: Rachel Yaffe

In recent months, the Department of Health and Human Services (HHS) and the Office of Civil Rights (OCR) have revved up their efforts in enforcing the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) through plans to conduct audits of covered entities (health care providers, health plans and health care clearinghouses) and business associates (persons or entities that perform certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, covered entities).

In March 2010, HHS contracted with consulting firm Booz Allen Hamilton to conduct a study of various audit methods. This study was completed in August 2010, but the results of the study have yet to be made public. However, on June 9, 2011, HHS awarded a $180,000 contract to Booz Allen Hamilton for "audit candidate identification." It is expected that Booz Allen Hamilton is engaged to identify a comprehensive list of covered entities and business associates throughout the United States.

On the following day, June 10, 2011, HHS awarded a $9.2 million contract to audit, tax and advisory firm KPMG to create an audit protocol and assist OCR in effectively conducting audits on select covered entities and business associates (presumably those identified by Booz Allen Hamilton in the above engagement) with regard to compliance with the Privacy and Security Rules. The audits of covered entities and business associates will entail the following:

- Site visits, including interviews with leadership (e.g., chief information officer, privacy officer, legal counsel, health information management/medical records director);
- Examination of physical features and operations;
- Consistency of process to policy; and
- Operations of compliance with regulatory requirements.

After each site visit, the auditor will then submit a report which will contain the following:

- Timeline and methodology of the audit;
- Best practices noted;
- Raw data collection materials (e.g., completed checklists and interview notes);
- Certification indicating the audit is complete;
- Specific recommendations for actions the audited entity can take to address identified compliance problems through a corrective plan of action, if any; and
- Description of future oversight recommendation.

The auditor will also submit a final report which will include the following:

- Identification and description of the audited entity (e.g., name, address, EIN, contact person);
- Methods used to conduct the audit;
- For each negative finding identified in the audit: the condition (defect or noncompliant status observed and evidence of each), criteria (clear demonstration that each finding is a potential violation of the Privacy or Security Rules), cause (reason that the condition exists and identification of supporting documentation used), effect (risk or noncompliant status that results from the finding), recommendations for addressing the findings and entity corrective actions taken, if any;
- Acknowledgment of any best practices or successes; and
- Overall conclusion.

The question on everyone's mind is "What can we do to prepare for a possible audit?" In light of these enhanced enforcement efforts by HHS and OCR, now is the time to do an internal audit of your organization's compliance with the Privacy and Security Rules. Do you have HIPAA policies and procedures in place? Are they updated periodically or are they sitting on a shelf collecting dust? Do you have Business Associate Agreements with your business

associates (if you are a covered entity) or covered entities (if you are a business associate)? Is the Business Associate Agreement form you are using HIPAA/HITECH Act compliant? Is your staff trained on how to identify (and how to then document and report) privacy and security breaches? Has your organization engaged in “test runs” to ensure that the policies and procedures that are in place actually work when conducted in a simulated setting? Policies and procedures that may look effective on paper may actually fail in a real time situation.

Whether you are a covered entity or a business associate, don’t wait until you are audited to get compliant. Get compliant now and ensure that you are prepared in the event an auditor comes knocking on your door.

Reprinted with permission from RBMA RadCast July 2011 issue.

http://www.rbma.org/Products_and_Resources/Legal_Resources/RBMA_Monthly_Legal_Update_Digest_July_2011.aspx