

HIPAA Audits Imminent

November 17, 2011

Jeff Miller

The HITECH Act requires HHS to periodically audit covered entities and business associates to ensure HIPAA compliance. Last week, OCR announced initial implementation of a pilot auditing program. The pilot program will audit 150 covered entities “to assess privacy and security compliance.” Audits should begin later this month (November 2011) and continue through December 2012.

HIPAA enforcement was a complaint-driven process until recently. The Health & Human Services (HHS) Office of Civil Rights (OCR), which enforces the HIPAA Privacy and Security Rules, would investigate an alleged violation only when an interested party made a complaint. With the HITECH Act, which was part of the American Recovery & Reinvestment Act of 2009 (aka the Stimulus Bill), that is no longer the case.

The HITECH Act requires HHS to periodically audit covered entities and business associates to ensure HIPAA compliance. Last week, OCR announced initial implementation of a pilot auditing program. The pilot program will audit 150 covered entities “to assess privacy and security compliance.” Audits should begin later this month (November 2011) and continue through December 2012. OCR has developed its audit protocols and will conduct a test of 20 audits between November 2011 and April 2012, when it will revise its protocols before completing the remaining 130 audits.

Audit Selection. The pilot program audits will focus on covered entities (healthcare providers, insurance companies, and healthcare clearinghouses). OCR will include business associates in future audits. OCR will choose entities for the pilot audits with the goal of making a broad assessment of the complex and diverse healthcare industry. OCR may audit covered individual and organizational providers of health services, as well as health plans of all sizes and types. OCR expects covered entities to provide auditors full cooperation and support consistent with the cooperation obligations imposed by the HIPAA Enforcement Rule.

OCR will inform entities selected for an audit in writing. The notice letter will introduce the audit contractor, explain the audit process and expectations, and make initial document and information requests focused on the entity’s privacy and security compliance efforts. OCR will expect the audited entity to provide the requested information within 10 business days.

On-Site Visit. In this pilot phase, every audit will include a site visit and result in an audit report. OCR has retained KPMG to conduct the audits on its behalf. OCR expects to notify selected covered entities between 30 and 90 days prior to the site visit. During site visits, which may last anywhere from 3 to 10 days, auditors will:

- interview key personnel (e.g., CIO, privacy officer, legal counsel, health information management/medical records director);
- examine the physical features, processes, and operations of the covered entity; and
- examine “consistency of process to policy” (in other words, whether the covered entity is following its own policies and procedures).

Covered entities should prepare now to provide documentation reflecting every policy, and to be able to demonstrate every procedure, relating to their implementation of the technical, physical, and administrative requirements of HIPAA.

Following the site visit, auditors will develop and share with the entity a draft report that will describe how the audit was conducted, what the findings were, and what actions the covered entity is taking in response to those findings. Support of each finding will include:

- Condition: the defect or non-compliant status observed, and evidence of each.
- Criteria: a clear demonstration that each negative finding is a potential violation of the Privacy or Security Rules, with citation.
- Cause: the reason that the condition exists, along with identification of supporting documents.
- Effect: the noncompliant status or risk arising from the finding.
- Recommendations: recommendations for addressing each finding.
- Correction: entity corrective action taken, if any.
- Acknowledgement: acknowledgement of any best practices or successes.

Opportunity for Remediation. Before the auditor finalizes the report, the covered entity will have 10 days to discuss concerns, provide comments, and describe corrective actions implemented to address issues identified. The final report submitted to OCR will incorporate the steps the entity has taken to resolve any compliance issues, as well as best practices of the entity. The whole process, start to finish, is expected to take between 60 and 90 days.

A rapid response to a remediation request could help avoid the substantial fines that can result if the covered entity is characterized by OCR as having exhibited “willful neglect.”

OCR intends to use these initial audits to help entities improve their compliance. OCR plans to use aggregated results of the audits to understand efforts entities are making to comply with specific aspects of the HIPAA Rules and to determine what types of technical assistance, and what corrective actions, are most effective. **However, should an audit report indicate a serious compliance issue, OCR is reserving the right to initiate a compliance review (including civil monetary penalties) to address the problem.**

This allowance for active remediation appears to have been the approach CMS and the HHS Office of Inspector General have taken in the few previous provider audits. That said, covered entities should take the potential for an OCR audit seriously and should seek to minimize exposure through pro-active, good-faith compliance efforts.

Changing Face of HIPAA Enforcement. CMS’s previous HIPAA enforcement efforts focused on education and voluntary remediation. Now, with an audit mandate and the availability of increased civil monetary penalties, OCR’s mission is changing to one of law enforcement, particularly with respect to health privacy

HIPAA Audits Imminent (Cont.)

rights. OCR's changing mission is also reflected by the HIPAA Enforcement Training sessions held nationwide for state attorneys general, two civil monetary penalty orders each greater than \$1 million, and three formal Resolution Agreements signed between February and July of this year. Given the recent TRICARE breach (loss of backup tape affecting 4.9 million service members, veterans, and their families) and the 301 Security Rule complaints and compliance reviews open as of September 30, 2011, expect to hear of more such activity.

Conclusion. Covered entities should confirm immediately that their HIPAA compliance program can withstand the depth and breadth of the anticipated audits. An audit will likely review all aspects of the Privacy Rule and the Security Rule, not merely a few select provisions.

For questions about HIPAA compliance, you may contact Jeff Miller or another member of H³GM's Healthcare Practice Group.