HHS Launches HIPAA Audit Program

PARKER | SMITH | FEEK

November 2011

Overview

The HITECH Act, a portion of The American Recovery and Reinvestment Act of 2009 (ARRA) requires the Department of Health and Human Services (HHS) to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards. To implement this requirement, The HHS Office for Civil Rights (OCR) is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance. OCR is the agency charged with HIPAA privacy and security compliance. Audits during the pilot phase will begin November 2011 and conclude by December 2012. It is anticipated that additional audits will continue after the initial pilot program.

OCR will use the audit program to assess HIPAA compliance efforts by a range of covered entities. Audits will examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's current compliance investigations and reviews. OCR plans to share information gleaned through the audit process and issue guidance targeted to observed compliance challenges.

Who Will Be Audited?

Every covered entity and business associate is eligible for an audit. OCR will audit as wide a range of types and sizes of covered entities as possible; covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses may all be considered for an audit. Business Associates will not be included in the initial audit pilot program but will be included in future audits.

How Will the Audit Program Work?

Entities selected for an audit will be informed by OCR of their selection and asked to provide documentation of their privacy and security compliance efforts. In this pilot phase, every audit will include a site visit and result in an audit report. During site visits, auditors will interview key personnel and observe processes and operations to help determine compliance. Following the site visit, auditors will develop and share with the entity a draft report; audit reports generally describe how the audit was conducted, what the findings were and what actions the covered entity is taking in response to those findings.

Prior to finalizing the report, the covered entity will have the opportunity to discuss concerns and describe corrective actions implemented to address concerns identified. The final report submitted to OCR will incorporate the steps the entity has taken to resolve any compliance issues identified by the audit, as well as describe any best practices of the entity.

What is the General Timeline for an Audit?

OCR expects to notify selected covered entities between 30 and 90 days prior to the anticipated onsite visit. Onsite visits may take between 3 and 10 business days depending upon the complexity of the organization and the auditor's need to access materials and staff. After fieldwork is completed, the auditor will provide the covered entity with a draft final report; a covered entity will have 10 business days to review and provide written comments back to the auditor. Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to address the problem. OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

Summary

It is expected that the majority of covered entities selected for the pilot audit program will be medical providers and insurance companies. However, based on the description of the audit process provided by HHS, it is likely that a number of employers will be included in the program relative to the health plans offered to their employees. Now would be a good time for employers who sponsor plans subject to the HIPAA privacy and security rules to review their existing HIPAA policies and procedures.