OCR Rolls Out HIPAA Audit Program

November 18, 2011

The U.S. Department of Health and Human Services' Office for Civil Rights released plans to audit 150 covered entities under its pilot HIPAA audit program. Covered entities should review HIPAA compliance policies and complete a security risk assessment to ready themselves for potential audit.

On November 8, 2011, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) published on its website the details of its pilot program to perform up to 150 audits of compliance with the privacy, security and breach notification standards (collectively, the Standards) adopted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) between November 2011 and December 2012 (the Pilot Audit Program).

Scope of the Audit Program

The Pilot Audit Program will include only HIPAA-covered entities, *i.e.*, health care providers, health plans and health care clearinghouses, and not their business associates, but OCR stated that business associates would be included in future audits. OCR implemented the Pilot Audit Program pursuant to Section 13411 of the HITECH Act, which requires OCR to conduct audits of covered entities and business associates to ensure they are in compliance with the Privacy and Security Rules and the Breach Notification standards. The audits will be conducted by KPMG, which was awarded the contract to develop the Audit Program and conduct the audits.

OCR intends to initially audit a sample of 20 covered entities to further hone and develop the audit protocols, which were created over a period of months. OCR anticipates that these initial audits and the subsequent evaluation of the Pilot Audit Program will be completed by the end of April 2012. OCR will then begin conducting the majority of audits of covered entities in accordance with the revised Pilot Audit Program protocols. OCR stated that it "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." While they will not be included in the initial 150 pilot audits, business associates will be included future audits after the pilot phase.

What the Audits Will Involve

All audits conducted during the Pilot Audit Program will include a site visit and result in a formal report. Covered entities selected for audit will receive a notification letter from OCR approximately 30 to 90 days prior to the site visit (OCR has provided a draft notification letter on its website). The letter will provide contact information for the auditor, explain the audit process and include an initial document request. The document request will require the covered entity to provide documentation of its efforts to comply with the Standards, which are expected to include, at a minimum, copies of the entity's privacy, security and breach notification policies and procedures and the security risk assessment required under the HIPAA security standards. Covered entities and business associates selected for an audit will have 10 business days to provide the requested documentation to OCR. The onsite visits may take anywhere between three to 10 days. During the site visits, auditors will interview personnel and observe the entity's practices. Thereafter, OCR will generate a draft report, which the covered entity will have 10 business days to review and provide written comments to the auditor. The auditor will then complete a final audit report within 30 business days and submit it to OCR. The final report will include the auditor's findings, the corrective steps the entity is taking to correct any deficiencies and a description of any best practices of the covered entity.

OCR stated that the Audit Program is primarily intended to improve its understanding of compliance efforts with particular aspects of the Standards, to determine what types of technical assistance should be developed and to determine what types of corrective actions are being developed. OCR will share best practices identified during the Pilot Audit Program and issue guidance on common compliance challenges, but it will not publish a list of the audited covered entities or any findings of an audit that could identify an audited entity.

However, in circumstances where an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited entity that could lead to civil money penalties. For more information about the civil money penalties authorized under HIPAA, see HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements.

How Companies Can Prepare

While OCR will only select a very small percentage of covered entities to be audited under the Pilot Audit Program, the Pilot Audit Program is representative of OCR's stepped up efforts to enforce and ensure compliance with the Standards. For more information on OCR's increased enforcement activity, see OCR Exercises its Enforcement Discretion. Accordingly, it would be prudent for covered entities to revisit their

policies and procedures for compliance with the Standards and ensure that they have completed and documented at least one security risk assessment consistent with the HIPAA security standards.

The McDermott Difference

McDermott Will & Emery has developed HIPAA privacy and security policies and forms updated for the HITECH Act to assist covered entities and business associates implementing and updating their HIPAA compliance programs. For more information, please contact an author or click here to learn more about our HIPAA practice and lawyers in your region.