Advisory

HIPAA PRACTICE GROUP | DECEMBER 2011

WIGGIN AND DANA

Counsellors at Law

If you have any questions about this Advisory, please contact:

Michelle Wilcox DeBarge
860.297.3702
mdebarge@wiggin.com

Jody Erdfarb
203.363.7608
jerdfarb@wiggin.com

OCR Begins HIPAA Audits

Last month, the United States Department of Health and Human Services' Office for Civil Rights (OCR) announced that its contractor, KPMG, will be conducting 150 HIPAA compliance audits from November 2011 to December 2012. OCR is required to conduct HIPAA audits pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH), which was passed by Congress as part of the much larger American Recovery and Reinvestment Act of 2009.

HITECH requires OCR to audit both covered entities and business associates to ensure full compliance with the HIPAA privacy and security rules as well as the breach notification rule. According to OCR, the 150 currently planned audits will be a pilot program including only covered entities. However, OCR plans to include business associates in future audits.

The Audit Process

OCR has posted an overview of the pilot audit program on its website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. While the initial audits will be conducted in accordance with the process currently described on the website, revisions are expected over time as the audits progress.

According to the current process, the OCR auditors will send selected entities a letter notifying them of the audit and requesting documentation of privacy and security compliance. Entities will be expected to provide all of the requested information with 10 days.

Every audit will also include a site visit, during which the auditors will interview key personnel and observe processes and operations. According to OCR, the auditors will give covered entities between 30 and 90 days notice of an anticipated site visit. The visits may take anywhere between 3 to 10 business days, depending on the size and complexity of the organization.

OCR auditors will then draft an audit report, which will be shared with the entity. The covered entity will have 10 business days to review the report, discuss any concerns with the auditors, and describe corrective actions implemented to address any identified problems. Within 30 days of receiving the entity's comments, OCR will then issue a final report, detailing all of the efforts taken to resolve any identified compliance issues. Interestingly, the audit report will also include a description of the covered entity's best practices.

Consequences of Noncompliance

On its website, OCR emphasizes that the primary purpose of the audits is to, "assess HIPAA compliance efforts by a range of covered entities . . . [and] examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews." However, OCR also notes that if a "serious" compliance issue is identified, a compliance review may be conducted to address the problem. Although not stated explicitly, if a covered entity fails to cooperate fully during the audit and/or if the auditors identify instances of noncompliance, the covered entity could face sanctions. Notably, the sample audit notification letter that OCR made available on its website states: "We expect . . . your full cooperation and support and remind you of your cooperation obligations under the HIPAA Enforcement Rule."

continued next page

WIGGIN AND DANA

Counsellors at Law

Prepare Now

OCR has not publicly identified which covered entities it will audit, but has stated that, "selections in the initial round will be designed to provide a broad assessment of a complex and diverse health care industry" and that, "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." Accordingly, all covered entities and business associates should prepare for the possibility of being selected for a compliance review as part of the pilot program.

Since audited entities must provide documentation of HIPAA privacy and security compliance within only 10 days, covered entities must ensure, prior to the time they are audited, that these materials are readily available and are up-to-date, accurate, and in full compliance with all applicable requirements. These include up-to-date policies and procedures and business associate agreements; documentation of HIPAA Security Rule compliance, including documentation of all risk assessments and implementation of appropriate safeguards that address all of the Security Rule standards; documentation of investigation and mitigation of all reported breaches; documentation of compliance with breach notification requirements; and documentation of employee training.

Also, since OCR will be conducting site visits, entities should ensure that all written policies and procedures are fully implemented as drafted. A HIPAA compliance program that is robust on paper, but that is not fully operational "on the ground," will not suffice. All employees should understand the rules applicable to their job responsibilities, be able to identify the privacy and security officers, and know how to report suspected problems.

Additionally, covered entities and business associates should closely monitor the OCR website for audit-related announcements. In fact, OCR stated that it will, "broadly share best practices gleaned though the audit process and guidance targeted to observed compliance challenges via," its website and other outreach portals.

In order to be fully prepared, covered entities should also assign a team to handle audit readiness. It will be essential to have a prepared team already in place by the time the audit begins. Entities should also consider conducting an internal audit of its HIPAA policies and procedures now to ensure that they are fully compliant.

~~~~~

In recent years, the federal government has made its intent to beef up HIPAA enforcement abundantly clear. In 2009, HITECH imposed new privacy and security requirements, expanded on those already in place, and most notably, required periodic HIPAA compliance audits and introduced enhanced penalties for noncompliance. To date, OCR has imposed penalties only in 8 cases; 5 of which were within the past two years. The start of OCR's new audit program is merely a continuation of this increased enforcement trend. Covered entities and business associates that have neglected to implement a robust HIPAA compliance program or that have been lax about HIPAA should improve their level of compliance without delay.
~~~~~