Cooley

January 18, 2012

Among other things, 2012 will be the year of the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") pilot audit program to assess compliance with the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules and Breach Notification standards. The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, required that HHS conduct periodic audits to monitor and ensure compliance with HIPAA. OCR will implement this requirement through a pilot program of 150 audits from November 2011 through December 2012, including an initial wave of 20 audits that will inform how the remaining audits will be conducted. OCR has established a **HIPAA Audit Program website**.

The pilot program of audits will have the following characteristics:

- The first 150 audits will apply to covered entities only. However, business associates will be included in future audits. As a reminder, covered entities are defined under 45 CFR 160.103 to include health plans, clearinghouses and certain health care providers, while business associates include persons or entities that perform "certain functions or activities that involve the use or disclosure of protected health information on behalf of, or [provide] services to, a covered entity." See **hhs.gov**.
- OCR will select the pilot program audited entities to reach a range of types and sizes of covered entities. As the Audit Program website describes, "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." OCR will not publish lists of audited entities or audit findings that clearly identify the audited entities.
- The audits are intended to generate general information about HIPAA compliance. The pilot program audits will assess not only compliance risks and vulnerabilities, but also best practices that OCR will share with the public. If a particular audited entity's audit report indicates a serious compliance issue, OCR may initiate a compliance review of the audited entity to address the problem.
- KPMG, which developed the audit protocols, will act as auditors and, in this pilot phase, will conduct a site visit for each audited entity and provide OCR with a report for each audited entity. The audited entity will have the opportunity to comment on a draft report. The final report will include the audit's methodology and findings, recommendations regarding the need for corrective action, corrective actions being performed by the audited entity, and best practices identified. The **OCR HIPAA Audit Protocol and Program Performance award notice** provides additional details on the audit protocols.
- The audit program will not affect covered entities' ongoing obligation to accept complaints from individuals about the covered entities' practices with respect to the HIPAA's Privacy and Security Rules and Breach Notification standards.

In 2012, the pilot audit program will affect covered entities as follows. 150 covered entities will be notified in writing that they have been selected for an audit. They will be required to provide requested information within 10 days and will be subject to an onsite visit within 30-90 days in accordance with timelines on the OCR Audit Program website. Business associates of covered entities that are selected for an audit may be affected in that their relationship with an audited entity will likely be scrutinized and the audited entity may request information from its business associates in order to respond to the audit.

The vast majority of covered entities and business associates will not be audited in 2012, but they can expect the audit program to provide lessons on compliance risks and best practices. They will likely need to update their staffing, policies and procedures, training, and business associate agreements accordingly. They may also gain insight into the audit methodologies and begin preparing for potential audits in 2013 and beyond.

If you have any questions regarding this update or how the HIPAA audit program could affect your company, please contact one of the attorneys listed above.