November 2011

HIPAA Privacy and Security Audits Begin:
Enforcement Measures May Follow

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services has begun the pilot phase of HIPAA privacy and security audits of health care providers, health insurers and health care clearinghouses ("covered entities") to assess HIPAA compliance efforts. While covered entities will be the focus of initial audits, business associates – organizations that provide services on behalf of covered entities and who as a result have access to protected health information (PHI) – will be included in future audits. Up to 150 covered entities will be subject to the initial audits, to be conducted by KPMG, LLP, the OCR audit contractor. Once notified in writing that the entity has been selected to be audited, entities will be required to provide requested information to KPMG, allow an on-site visit, and respond to the auditor's initial report. Although the OCR says that audits are primarily a "compliance improvement activity," the OCR may take further action if the audit uncovers serious HIPAA compliance issues. As a result of this audit process, all covered entities and their business associates should review their HIPAA privacy and security practices.

The HIPAA privacy and security audits were mandated under the American Recovery and Reinvestment Act of 2009. The OCR must perform periodic audits to ensure covered entities and business associates are complying with the HIPAA privacy and security rules as well as the breach notification standards. The pilot audits will conclude by December 2012. The audits are designed to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not be discovered through OCR's complaint investigations. However, it is important to note that while OCR emphasizes these audits will aid in overall HIPAA compliance, it leaves open the door to impose sanctions on those entities that have serious HIPAA compliance problems.

By law, covered entities and business associates are required to cooperate with auditors. Those selected for an audit will first receive written notification and will be asked to provide documentation of their privacy and security compliance efforts. In the pilot phase, every audit will include a site visit and result in an audit report. During the site visit, auditors will interview key personnel and observe processes and operations to determine compliance. A draft audit report will be prepared and the covered entity will have the opportunity to discuss concerns and describe corrective actions implemented to address concerns identified by auditors. The final report will be submitted to OCR, who may take further action, if compliance issues are serious.

Once a covered entity receives notification that it has been selected for an audit, it will have 10 business days to provide the requested information. It is expected that covered entities will receive between 30 and 90 days advance notice of the onsite visit. Onsite visits are expected to last between 3 and 10 business days, depending on the covered entity's complexity and the auditor's need to access materials and staff. After fieldwork is completed, the covered entity will receive a draft report and will have 10 business days to provide a response and provide a plan to address any compliance issues uncovered. The auditor (KPMG) will then have 30 business days to submit the written audit report to OCR.

While OCR claims it will use the audits to determine overall compliance with the HIPAA privacy and security rules and uncover best practices, it reserves the right to take enforcement action against covered entities for serious HIPAA issues. Because of this possibility, all covered entities and business associates should review their privacy and security policies and practices and be prepared for an audit. While the pilot audits are initially limited to 150, the audit program will expand in future years and will become a standard feature that covered entities and business associates will have to contend with.