CONTACT

Stephen D. Rose
Practice Group Chair
206.816.1375
srose@gsblaw.com

HHS AWARDS CONTRACT TO CONDUCT HIPAA AUDITS

November 2011

On June 10, 2011, KPMG was awarded a $9.2 million contract by the Department of Health and Human Services (HHS) to develop HIPAA[1] audit protocols and then conduct audits based on those protocols of HIPAA Covered Entities and Business Associates. The HIPAA audit protocols will be developed by KPMG under the guidance of HHS staff.

HIPAA Audits Required by the HITECH Act

Currently, HHS conducts HIPAA investigations through the Office for Civil Rights (OCR). Since the inception of HIPAA, OCR has initiated investigations of possible HIPAA violations based on complaints it has received. The Health Information Technology for Economic and Clinical Health (HITECH) Act[2] mandates that HHS conduct audits of Covered Entities and Business Associates to ensure that they are complying with the HIPAA Privacy and Security Rules.

Audit Reporting Requirements

The contract issued to KPMG does include some mandated report items and actions. Site visits must be conducted as part of every audit. During the site visit the auditors are required to interview management personnel such as the organization's Chief Information Officer, Privacy Officer, legal counsel, and medical records director.

After each site visit the auditor must submit an "Audit Report." At a minimum, the Audit Report must contain the following:

- A timeline and methodology of the audit;
- Best practices noted;
- Raw data collection materials such as completed checklists and interview notes;
- Certification stating that the audit is complete; and
- Specific recommendations for action

---

1 *Health Insurance Portability and Accountability Act of 1996.*

2 *The HITECH Act was passed into law as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5). ARRA was enacted on February 17, 2009.*

Next, the auditor must prepare a "Final Report." At a minimum, the Final Report must contain the following:

- Identification and description of the audited entity (including full name, address, EIN, and contact person);
- Methods used to conduct the audit;
- For each finding:
    - Condition: the defect or noncompliant status observed, and evidence of each;
    - Criteria: a clear demonstration that each negative finding is a potential violation of the Privacy or Security Rules, with citation(s);
    - Cause: the reason that the condition exists, along with identification of supporting documentation used;
    - Effect: the risk of noncompliant status that results from the finding;
    - Recommendations for addressing each finding; and
    - Entity corrective action taken, if any.
- Acknowledgment of any best practice(s) or success(es); and
- Overall conclusion paragraph.

All of the above items can be found in the federal government synopsis of the KPMG contract which can be found at:

https://www.fbo.gov/index?s=opportunity&mode=form&id=9e045aa4f7e6f8499c5b6f74d5b211e9&tab=core&_cview=0

Conclusion

HIPAA audits commence in November of 2011, so you should prepare for them immediately. While the likelihood of any one organization being audited is small, the possibility now exists. Now would be a good time to review and update your HIPAA Policies and Procedures. If you have not performed your annual Risk Assessment, now would be a good time to do it. The contract requires that at least 150 audits be conducted before December 31, 2012.