OBER | KALER
Attorneys at Law

2011 Issue 4

www.ober.com

SPECIAL FOCUS: HIPAA/PRIVACY

HIPAA Audits Are Coming: KPMG Contracted to Perform 150 Audits Through 2012

By: James B. Wieland and Joshua J. Freemire

You can't run and you can't hide — HIPAA audits are coming. HHS, through the Office of Civil Rights (OCR) recently named KPMG as the recipient of a $9.2 million contract to develop a HIPAA auditing protocol and conduct audits on 150 covered entities and business associates before December 31, 2012. An additional $180,000 contract has been awarded to Booze Allen Hamilton for "OCR HIPAA Audit Candidate Identification." If they identify you, are you prepared?

Section 13411 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (passed as part of the American Recovery and Reinvestment Act of 2009), required HHS to conduct periodic audits of providers and business associates to ensure their compliance with "this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of" the HITECH Act. The HITECH Act itself provides no explanation of what an audit might entail, but the OCR solicitation itself provides some details. According to the solicitation, required audit work will include a site visit, including:

- Interviews with leadership (e.g., CIO, Privacy Officer, legal counsel, health information management / medical records director);
- Examination of physical features and operations;
- Consistency of process to policy; and
- Observation of compliance with regulatory requirements.

KPMG will also be required to prepare a written report of the audit, consisting of:

- The audit timeline and methodology
- Best practices noted
- Raw data collection materials (including interview notes and completed checklists)
- A certification the audit is complete
- "Specific recommendations" for actions the audited entity may take to address identified compliance problems "through a corrective action plan"
- Recommendations to the OCR Contracting Officer's Technical Representative (COTR) regarding the continuing need for corrective action, if any, and a description of future oversight recommendations

For each finding, the audit report must provide:

- Condition: the defect or noncompliance observed, and the evidence of each
- Criteria: a clear demonstration that the negative finding is a potential violation of the Privacy or Security Rules, with relevant citations
- Cause: the reason the identified noncompliance exists, and an identification of the supporting documentation demonstrating it exists
- Effect: the risk caused by the identified potential noncompliance
- Recommendations to correct negative findings
- Corrective actions taken (if any)
- Acknowledgement of best practices or successes
- An overall "conclusion paragraph"

HHS OCR's solicitation does not explain whether the reports will be made public, but the OCR's general trend towards disclosure of settlements and data breaches indicates that audit findings will, in some form, be made generally available. Though no strict timeline for the audits is established, HHS OCR's solicitation explains that it anticipates the completion of 150 audits by December 31, 2012.

Ober|Kaler's Comments

What the solicitation does not answer, of course, is how HHS OCR will respond to negative audit findings. Presumably, entities that are found to be substantially out of compliance will be further investigated, perhaps penalized, and asked to enter into a Corrective Action Plan (CAPs, as discussed in detail in the article, "Corrective Action Plans Can Mean Significant Compliance Monitoring Requirements," can entail burdensome reporting obligations, or even outside monitors, for a significant period of time.)

Providers should take steps to prepare now, starting with their privacy and security policies and procedures. HIPAA provides significant discretion to tailor such policies and procedures to the size, complexity and resources of each individual provider. It is essential that providers take heed of the audit solicitation's note that "consistency of policy to practice" will play a key role in determining compliance. One simple step that every provider can take is to review their existing policies and ask themselves, "Is this really how we do things?" and "Does this cover everything we do with PHI?" Technology, and the HITECH Act amendments to HIPAA, have likely outpaced policies and procedures that were drafted when the Privacy Rule became effective in 2003 and have not been reviewed and revised since then.