Davis Wright Tremaine LLP

And the New HIPAA Cop Is … HHS Appoints Contractor to Conduct HIPAA Privacy and Security Audits

By Adam H. Greene

June 05, 2011

On June 10, 2011, the Department of Health and Human Services (HHS) awarded to KPMG a $9.2 million contract to create an audit protocol and then audit covered entities' and business associates' compliance with the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The contract calls for as many as 150 audits of entities varying in size and scope before Dec. 31, 2012.

In light of the large numbers of HIPAA covered entities and business associates, the likelihood of being audited will be small. Nevertheless, now is a good time for covered entities and business associates to review their HIPAA privacy and security programs, ensure that their documentation is up to date, and assess whether their programs are effectively protecting protected health information.

The HITECH Act's audit program

HHS, through the Office for Civil Rights (OCR), historically has investigated potential violations of the Privacy Rule (and more recently the Security Rule) based on the receipt of complaints. OCR also has initiated some "compliance reviews," proactively initiating investigations of covered entities (often in response to media reports indicating noncompliance).

Section 13411 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, requires HHS to, additionally, conduct periodic audits to ensure that HIPAA covered entities and business associates are complying with the Privacy and Security Rules.

HHS contracted with Booz Allen Hamilton in March 2010 to conduct a study of different audit methodologies. Booz Allen completed the contract in Aug. 2010, but HHS has not made the resulting report public.

Two new audit contracts

In June, HHS awarded two contracts related to the HIPAA audit program. One contract, which HHS awarded to Booz Allen Hamilton on June 9, 2011, for $180,000, is for "audit candidate identification." While limited information has been released about this contract, it is presumably for the purpose of identifying the universe of covered entities and business associates. Especially with respect to business associates, it may prove impossible for Booz Allen to generate a truly comprehensive list of candidates.

The second contract, awarded to KPMG for $9.2 million, requires the contractor to develop an audit protocol and then conduct privacy and security audits.

Every audit would include a site visit and an audit report. According to the available contract synopsis, the site visits include interviews with leadership (e.g., chief information officer, legal counsel, health information management/medical records director); examination of physical features, operations, and adherence to policies; and observation of compliance with HIPAA regulatory requirements.

The audit report will include a timeline and methodology of the audit, best practices noted, raw data from the audit such as completed checklists and interview notes, and a certification indicating that the audit is complete. The report must include specific recommendations for actions the audited entity can take to address identified compliance problems through a corrective action plan. The report also must include recommendations to HHS regarding the continued need for corrective action, if any, and a description of future oversight recommendations.

KPMG is required to provide a final report for each audit that includes, at a minimum:

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

The contract synopsis indicates that HHS anticipates 150 audits, but recognizes that the nature of the work makes it impossible to anticipate the level of effort needed (i.e., there may be more or fewer audits based on the amount of time and resources that each audit involves). The contract is firm fixed price, meaning that payment to KPMG will not be based on whether audits result in resolution agreement payments or civil money penalties. The audit contract is through Dec. 31, 2012, so the audits will occur over a relatively short period of time. Since the audit program is being funded through the HITECH Act, it is not clear whether the audit program will continue after HITECH Act funds expire in 2012.

A few answers, a lot of questions

The awarding of the audit contracts raises as many questions as it answers. We do not know the scope of the audits, such as whether KPMG will review general compliance with the Privacy and Security Rules or whether the audits will be focused on specific issues. Once Booz Allen Hamilton completes its contract to identify audit candidates, we do not know how entities will be selected for audit (the contract synopsis suggests some level of stratification, indicating that entities of different size and scope will be selected, but we do not know to what degree selection will be through a random process). We do not know what will happen if an entity is selected for audit and it has an existing relationship with KPMG; KPMG may need to use a subcontractor to conduct such audits. Most importantly, we do not know whether the audit program will be used as an enforcement tool (leading to resolution agreements or civil monetary penalties), or whether it will be used strictly as an educational tool to improve general compliance.

Currently, we only have access to the synopsis of the KPMG contract. As the contract itself becomes available, some of these questions may be answered. Most questions, however, will only be answered once KPMG creates an audit protocol and begins conducting audits.

Next steps

The chances of being selected for audit are low, but some covered entities (and possibly business associates) will become the unlucky few. In the meantime, covered entities and business associates should assess their privacy and security programs, including breach detection and notification, to prepare for the possibility of an audit.

Covered entities may wish to focus on checking that policies and procedures are up to date, rather than merely a binder sitting on a shelf, and ensure that the workforce has been appropriately trained (especially newer staff). Covered entities and business associates also may wish to do their own site visits to see that policies have been implemented among staff and that they are effective in protecting privacy. Some seemingly good privacy policies fail in the face of practical realities, such as human error, limited staff time, and limited resources.

Covered entities and business associates should also ensure that their security risk analysis is up to date, reflecting lessons learned since the Security Rule went into effect, and reflecting changes in technology and costs. For example, if you have a 2005 risk analysis stating that encryption of laptops is too expensive, it may be wise to update your analysis based on changes in costs.

While it may be impossible to achieve a perfect, fully compliant privacy and security program that will be audit-proof, now is a good time to tackle some of these bigger issues that oftentimes lead to noncompliance.