HHS Steps up HIPAA Audits: Now Is the Time to Review Security Policies and Procedures

By Adam H. Greene

Now Is the Time to Review Security Policies and Procedures

In June 2011 the Department of Health and Human Services awarded KPMG a $9.2-million contract to create an audit protocol and audit organizational compliance with the HIPAA privacy and security requirements.[1] The contract calls for as many as 150 audits of covered entities and business associates before December 31, 2012.

The HHS Office for Civil Rights (OCR), the agency responsible for administering and enforcing the privacy and security rules, has indicated major violations uncovered by the audits may lead to formal enforcement measures (such as settlement agreements or civil monetary penalties).[2] In preparation for these audits, covered entities and HIM professionals need to be proactive and review organizational privacy and security compliance programs to ensure they are effectively protecting health information.

The HITECH Act's Audit Program

The HITECH Act mandates that HHS conduct periodic privacy and security audits of HIPAA covered entities and business associates. In response to this mandate, HHS recently awarded two contracts related to the HIPAA audit program.

HHS awarded a $180,000 contract to Booz Allen Hamilton on June 9, 2011, for "audit candidate identification."[3] The purpose of this contract is to identify a means for HHS to create and maintain a comprehensive inventory of all HIPAA covered entities subject to these audits. The contract runs through October 2012.

The contract awarded to KPMG requires the contractor develop an audit protocol and conduct privacy and security audits. The audit protocol covers both the HIPAA privacy and security rules. Audits will assess whether a covered entity has comprehensive policies and procedures and has implemented them consistent with the HIPAA rules.[4] According to the contract, every audit will include a site visit and an audit report.

Site visits will be conducted by audit teams of three to five auditors (or two to three auditors for small, noncomplex practices) with expertise in compliance auditing, HIPAA privacy and security, and IT auditing.[5] The visits will include interviews with leadership (e.g., chief information officer, legal counsel, health information management director); examination of physical features, operations, and adherence to policies; and observation of compliance with HIPAA regulatory requirements. The auditors are expected to issue an advanced request for documentation from the covered entity so that the audit team can prepare for the site visit.[6]

The final report for each audit is required to include, at a minimum:

- Identification and description of the audited entity (including full name, address, employer identification number, and contact person)
- The methods used to conduct the audit
- The defect or noncompliant status observed (including evidence)
- A clear demonstration that each negative finding is a potential violation of the privacy or security rules, with citation
- The reason that the condition exists, along with identification of supporting documentation used
- The risk or noncompliant status resulting from the finding
- Recommendations for addressing each finding

- Entity corrective actions taken, if any
- Acknowledgment of any best practices or successes
- An overall conclusion paragraph

While the HITECH Act refers to audits of both covered entities and business associates, OCR has indicated that the primary focus will be on covered entities.[7] The contract calls for the protocol to reflect the specific requirements that apply to each type of covered entity. The contract requires the protocol include the flexibility to evaluate a wide variety of entities that have widely varying resources.

OCR has not yet indicated whether the audit protocol will be made public.

Major Violations May Lead to Enforcement

One of the biggest questions is whether these audits will be focused on gauging the state of compliance or whether HHS will use them primarily as a tool to penalize covered entities. Early indications are that OCR will be taking the former approach.

Susan McAndrew, the deputy director for privacy at OCR, has indicated that the purpose of the audits will be to measure compliance in the absence of a precipitating incident and as a tool for educating the public.[8] If an entity is audited and potential violations are found, the audited entity should not assume that it will need to enter into a settlement agreement or that a civil monetary penalty will be imposed.

Nevertheless, while the focus of the audits will be prevention and education, McAndrew has also stated that the discovery of major violations may lead to formal enforcement. Auditors will likely refer discoveries of "serious noncompliance" to OCR for investigation and enforcement.

Payment to KPMG will not be based on whether audits result in resolution agreement payments or civil money penalties.

The Audit Program's Future

The audit contract is through December 31, 2012, so the audits will occur over a relatively short period of time. Once the audit protocol is completed, the contractor will conduct approximately 20 audits. After these initial audits, the contractor will receive feedback from HHS and the audit teams. It will then revise the protocol to address any concerns, implement improvements, and conduct the remainder of the audits.

McAndrew has indicated that development of the protocol is expected to occur through October 2011. The protocol will be tested in the initial set of audits through the end of January 2012, and the remainder of the audits will occur through December 2012.[9]

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. While budgets around the federal government are expected to be tight, the HITECH Act authorizes OCR to retain settlement and civil monetary penalty funds, and such funds could be used to conduct future audits.

There are numerous indications that if the audit program is considered successful, OCR will continue past 2012. The Booz Allen Hamilton contract for identifying audit candidates continues through October 2012, suggesting that the results will be used in future audits. The KPMG contract provides that the audit protocol will consist of modules that could lead to more issue-focused audits in the future.

Next Steps

The chances of being selected for audit are low; nevertheless some covered entities will find themselves audited. In preparation for the possibility of an audit, HIM professionals should work with colleagues to assess their privacy and security programs, including breach detection and notification.

Covered entities may wish to focus on checking that policies and procedures are up to date and ensure the workforce has been appropriately trained, especially newer staff. Covered entities also may wish to do their own mock site visits to ensure

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.

Organizations should focus resources on eliminating potential major violations, such as any lack of safeguards for large repositories of information or systematic failures that preclude individuals from exercising their privacy rights. While it may be impossible to achieve a perfect, fully compliant, audit-proof privacy and security program, now is a good time for HIM professionals to tackle some of the bigger issues that often lead to noncompliance.

Notes

1. Department of Health and Human Services (HHS). HHS Task Order HHSP233201100252G, Contract GS-3F-8127H. Audit Contract.
2. Anderson, Howard. "McAndrew Explains HIPAA Audits." *Healthcare Info Security*, July 15, 2011. www.healthcareinfosecurity.com/podcasts.php?podcastID=1190.
3. HHS. HHS Task Order HHSP23337007T. Contract HHSP23320095627WC.
4. Audit Contract, 6.
5. Audit Contract, 10–11.
6. Anderson, Howard. "McAndrew Explains HIPAA Audits."
7. Ibid.
8. Plank, Kendra Casey. "HIPAA Audits More Preventative Than Punitive, HHS Official Says." *BNA Health IT Law and Industry Report*, August 22, 2011. www.bna.com/hipaa-audits-preventive-n12884903205.
9. Greene, Adam, Cliff Baker, and Susan McAndrew. "The Upcoming OCR HIPAA Audit Program-What to Expect and How to Prepare." Web conference, July 28, 2011. www.dwt.com/Events?find=427233.

Adam H. Greene (adamgreene@dwt.com) is a partner at Davis Wright Tremaine LLP.

Article citation:
Greene, Adam H. "HHS Steps up HIPAA Audits: Now Is the Time to Review Security Policies and Procedures" *Journal of AHIMA* 82, no.10 (October 2011): 58-59.