Thomas D. Bixby
Law Office LLC
Legal Advice for Health Plans

PRIVACY LAW ALERT
March 18, 2012

OCR Plans 130 HIPAA Privacy/Security Audits By Year End

Covered Entities Urged to Prepare with "Robust" Compliance Assessment

The second phase of the Department of Health and Human Services Office for Civil Rights' (OCR's) audits of covered entities' HIPAA compliance are to begin in earnest over the next few months, with as many as 130 audits to be completed by the end of the year. This initial group of audits is a pilot program, with more audits expected in subsequent years. Although only covered entities will be targeted this year, business associates may also be the subject of audits in later years. The audits are required by the HITECH Act and will review compliance with the HIPAA Privacy and Security Rules and the HITECH Act's Breach Notification Rule.

Last year, OCR developed audit protocols for its initial set of audits and undertook 20 audits to test the protocols beginning in November. OCR will review and revise its audit protocols based on experience gained in these audits and then begin the process for 2012 audits as early as April (see timeline for OCR audit program on next page). OCR plans to use audit results "to examine mechanisms for compliance, identify best practices and discover [previously unidentified] risks and vulnerabilities." OCR expects to "broadly share best practices gleaned through the audit process and [to develop] guidance targeted to observed compliance challenges." Notwithstanding these benign expectations, OCR "will assess whether to open a separate compliance review in cases where an audit indicates serious compliance issues."

Covered entities will be asked for documentation of their compliance efforts, including written policies and procedures. Documentation will be required within ten days of the auditors' request. Auditors will then conduct a site visit, during which they will "interview key personnel and observe processes and operations to help determine compliance." The site visits will last from 3-10 days "depending upon the complexity of the organization and the auditor's need to access materials and staff." Once covered entities receive a draft audit report, they will have ten days to review the report and provide comments, after which the auditor will prepare a final report (see OCR's audit timeline table on page 3).

The OCR hired KPMG LLP to conduct the audits. In a presentation on the OCR audits last month,[1] KPMG's National HIPAA Services Director discussed the audits. In the presentation, he recommended that covered entities be prepared for the possibility of an

[1] The presentation was at an American Bar Association Conference on February 17, 2012.

audit by conducting a "robust" privacy and security assessment and a reassessment once or twice per year. In addition, he recommended that covered entities increase monitoring programs, include business associates in their privacy and security assessments, and train employees on HIPAA annually.

Increased Scrutiny and Enforcement

The audit program is one aspect of increased scrutiny of covered entities' compliance with the Privacy and Security Rules arising from the HITECH Act. In addition to the requirement that OCR audit covered entities, the HITECH Act granted the OCR the

Timeline for OCR Audit Program

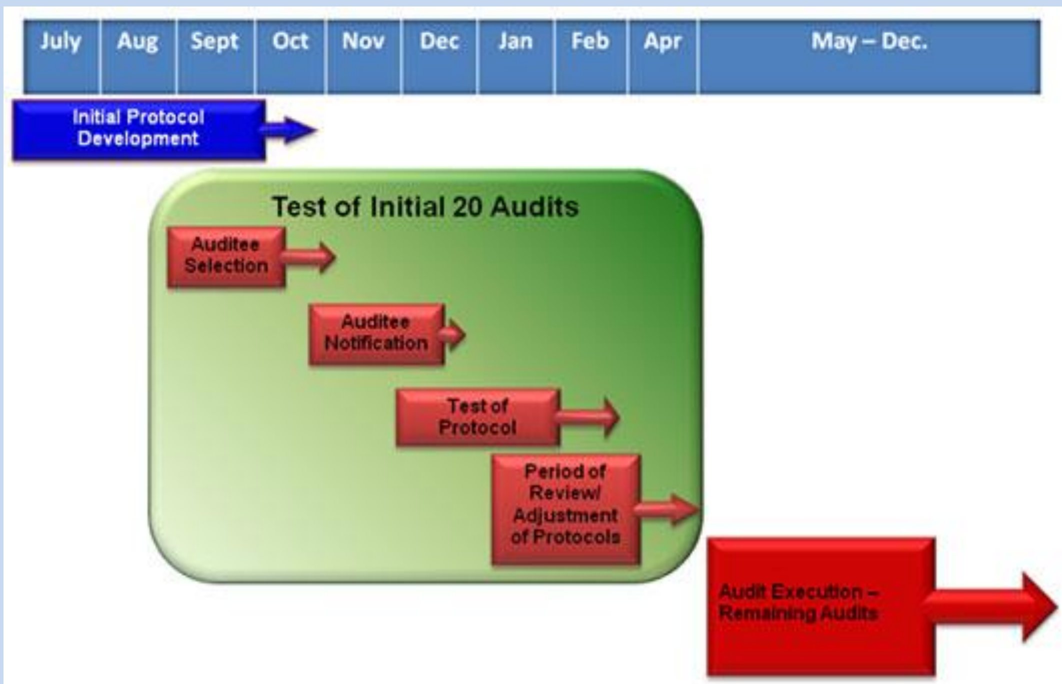

Table reproduced from OCR website, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

authority to impose significantly greater Civil Money Penalties and State Attorneys General the authority to enforce Privacy, Security, and Breach Notification requirements (click here for my Health Law Alert on HIPAA Enforcement Rule). In addition, notices provided to affected individuals, the Department of Health and Human Services, and (in some cases) the public under the Breach Notification Rule have served to give privacy and security compliance issues a higher public profile.

Indeed, last week the OCR engaged in its first enforcement action under the HITECH Act's enhanced penalty scheme. The OCR settled potential violations of the HIPAA Privacy and Security Rules arising out of the theft of 57 computer hard drives containing unencrypted protected health information. The parties agreed to a $1.5 million payment and a "corrective action plan to address gaps in [the health plan's] HIPAA compliance program.

Privacy and Security Assessments

Health plans (as well as business associates) should consider conducting an assessment of their privacy and security program compliance to determine whether policies and procedures adequately address the Privacy and Security Rules requirements as well as to ensure that changes required by the HITECH Act are properly implemented. For more information, please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com.

* * * * * * * * * *

OCR's Audit Timeline

Table reproduced from OCR website, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

Thomas D. Bixby Law Office LLC
(608) 661-4310 | www.tbixbylaw.com