EPSTEIN BECKER GREEN | HEALTH CARE & LIFE SCIENCES CLIENT ALERT

Thought Leaders in Health Law®

HHS Publishes Roadmap for HIPAA Audits

by Arthur J. Fried and Leah A. Roffman

August 2012

One of the less well-known provisions of the Health Information Technology for Economic and Clinical Health (or "HITECH") Act[1] is the requirement that the U.S. Department of Health and Human Services ("HHS") periodically conduct audits to ensure that Covered Entities[2] and their Business Associates[3] are complying with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[4] In November 2011, the HHS Office for Civil Rights ("OCR") launched the pilot phase of its HIPAA compliance audit program ("Audit Program"), selecting 115 entities nationwide to undergo privacy and security audits. While the pilot phase is not scheduled to wind up until December 2012, OCR recently made the protocol[5] guiding these compliance audits publicly available. By identifying individual areas of evaluation, defining the applicable performance criteria, and specifying how auditors will assess compliance with each, the protocol provides a comprehensive and extremely useful roadmap for entities anticipating an OCR audit and all other entities seeking to ensure HIPAA compliance. All Covered Entities and Business Associates should take note, as OCR recently announced that the Audit Program will likely continue through 2014.

Background of the Audit Program

The Audit Program analyzes processes, controls, and policies of entities covered by HIPAA in order to assess compliance efforts, identify best practices, and discover key areas of risk and vulnerability. Although OCR reserves the right to launch a formal investigation if an audit reveals a serious compliance problem, OCR has also stated that such investigations are not the goal of the Audit Program. By the end of 2012, OCR expects to complete its

[1] Pub. L. No. 111-5 (2009), at § 13000.
[2] A "Covered Entity" is defined by HIPAA as: (i) a health care provider who transmits health information in electronic format in connection with HIPAA-covered transactions, (ii) a health plan, or (iii) a health care clearinghouse. 42 C.F.R. § 160.103.
[3] A "Business Associate" is defined by HIPAA as an entity that provides services for or on behalf of a Covered Entity involving the use of individually identifiable health information. 42 C.F.R. § 160.103.
[4] Pub. L. No. 104-191 (2003).
[5] Available online at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

audit of the 115 entities involved in the pilot phase, all of which have already been notified and are defined by HIPAA as "Covered Entities." As indicated above, OCR has announced that the Audit Program will likely continue following the pilot phase, at which point it will probably be expanded to include Business Associates of Covered Entities.

Generally, an audit begins with OCR sending a written notification and document request list to the entity. The entity can then expect a site visit, during which auditors interview employees, review documentation of HIPAA policies and procedures, and observe HIPAA compliance. Following the site visit, the auditors develop a draft report, which the entity may review and comment on prior to submission to OCR. The final report sent to OCR includes any compliance issues identified, corrective action steps undertaken by the entity or recommended by the auditor, and any best practices of the entity.

Audit Program Protocol

The protocol was developed over the first 20 audits, and OCR expects to further modify and improve it as the remaining audits progress. In its current form, the protocol sets forth 165 areas of performance evaluation; for each such area, it cites the relevant HIPAA regulation, identifies the primary action needed to comply, and states how auditors will assess compliance.

Of these areas of performance evaluation, 88 relate to the HIPAA Privacy and Breach Notification Rules. Pursuant to the protocol, auditors will ensure that the entity complies with HIPAA requirements regarding, by way of example:

- confidential communications with individuals;
- disclosures of health information to family members and close friends;
- disclosures of health information for research purposes;
- individuals' rights to access and amend their health information;
- risk assessment following a potential security breach to determine whether significant harm has occurred; and
- notifications to individuals, the media, and HHS following a security breach.

The remaining 77 areas of performance evaluation included in the protocol relate to the HIPAA Security Rule. Auditors will examine entities' compliance with HIPAA security requirements regarding, by way of example:

- periodic and accurate assessments of security risks;
- implementation of a sanction policy to address system misuse and abuse;
- implementation of a plan to respond to and report security incidents;
- implementation of a data backup and disaster recovery plan;
- development of a system for the final disposal of electronic health information; and
- assignment of unique identifiers to all system users.

Some of the themes recurring throughout the protocol include periodic compliance assessments, maintenance of policies and procedures to reflect changes in the entity's environment, creation and retention of HIPAA-related documentation, and regular training of relevant employees.

Key Considerations

The Audit Program is just one piece of evidence that we have entered a period of heightened HIPAA scrutiny and enforcement. OCR has publicized not only both the Audit Program and its impression that many Covered Entities are out of compliance with HIPAA but also recent enforcement actions outside the Audit Program. For example, in June 2012, OCR entered into a settlement with the Alaska Medicaid Agency, which suffered a breach of unsecured protected health information when a USB drive was stolen from an employee's car. Upon investigation, OCR discovered that the Alaska Medicaid Agency did not (i) conduct a risk analysis, (ii) complete appropriate security training, or (iii) implement necessary device and media controls. As a result, OCR fined the Alaska Medicaid Agency $1.7 million.

The protocol is a valuable tool that offers insight into OCR's view on HIPAA compliance. Both Covered Entities and Business Associates would be well advised to utilize the protocol as a reference document to ensure that their HIPAA compliance programs are up to date and their processes are effective. Taking a proactive approach to improving policies, implementing procedures, and training employees will not only mitigate the effects of an OCR audit but also help to preclude HIPAA violations and subsequent investigations.

* * *

This Client Alert was authored by **Arthur J. Fried** and **Leah A. Roffman**. *For additional information about the issues discussed in this Client Alert, please contact one of the authors or the Epstein Becker Green attorney who regularly handles your legal matters.*