Connecticut Law Tribune

May 14, 2012

An ALM Publication

HEALTH LAW

Feds Step Up HIPAA Compliance Audits

Unprepared entities risk being hit with hefty financial penalties

By MICHELLE WILCOX DeBARGE and JODY ERDFARB

The Health Insurance Portability and Accountability Act (HIPAA) has fundamentally changed the health care industry's privacy and security practices. However, the federal government's enforcement efforts historically have been complaint-driven and sporadic. As a result, HIPAA-covered entities and business associates typically have failed to make compliance a priority. In fact, in 2008, the federal Department of Health and Human Services Office of Inspector General published a report criticizing the government's HIPAA oversight, concluding that, "reliance on complaints alone was ineffective" for identifying noncompliance.

The era of reactive and passive enforcement has ended, however. In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act, which included enhanced HIPAA enforcement provisions and increased penalties for noncompliance. Most notably, HITECH required the federal Department of Health and Human Services' Office for Civil Rights (OCR) to conduct periodic HIPAA compliance audits. HITECH also imposed new HIPAA privacy and security requirements and expanded those already in place. Since HITECH's enactment, the Office for Civil Rights has imposed civil monetary penalties in seven cases, whereas it did so only in two cases between 2003 and 2010.

Michelle Wilcox DeBarge

Jody Erdfarb

In November 2011, the office began conducting the now-mandatory HIPAA compliance audits through an initial audit pilot project. Although HITECH requires OCR to audit both covered entities and business associates, the pilot audit program includes only covered entities. OCR has not publicly identified which covered entities it will audit, but stated that, "selections in the initial round will be designed to provide a broad assessment of a complex and diverse health care industry" and that, "OCR will audit as wide a range of types and sizes of covered entities as possible . . ." OCR plans to include business associates in future audits.

Audit Process

OCR has posted an overview of the pilot audit program on its web site at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. Initial audits will be conducted in accordance with the process currently described on the website, but revisions are expected over time.

The current process provides that selected entities will receive a letter requesting the

Michelle Wilcox DeBarge is a partner in Wiggin and Dana's Health Care Department, based in Hartford. Her e-mail address is mdebarge@wiggin.com. Jody Erdfarb is an associate in the Stamford office of the firm's Health Care Department. Her e-mail address is jerdfarb@wiggin.com.

production of documentation of HIPAA compliance within 10 days. Auditors will also conduct site visits to interview key personnel and observe operations. According to OCR, the auditors will provide between 30 and 90 days notice of an anticipated site visit, and the visits may take anywhere between three to 10 days, depending on the size and complexity of the organization.

OCR auditors will then draft an audit report, and the covered entity will have 10 days to submit a written response. Within 30 days of receiving the entity's comments, OCR will issue a final report.

On its web site, OCR emphasizes that the primary purpose of the audits is to, "assess HIPAA compliance efforts by a range of covered entities . . . [and] examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews." However, OCR also notes that if a "serious" compliance issue is identified, a compliance review may be conducted to address the problem.

Although not stated explicitly, if a covered entity fails to cooperate fully during the audit and/or if the auditors identify instances of noncompliance, the covered entity could face sanctions. Notably, the sample audit notification letter that OCR made available on its web site states: "We expect . . . your full cooperation and support and remind you of your cooperation obligations under the HIPAA Enforcement Rule." This is not a minor point as the largest civil monetary penalty imposed to date by OCR against a covered entity, in the amount of $4.4 million, was mainly as a result of the covered entity's failure to cooperate with OCR's investigation.

Prepare Now

Because OCR HIPAA audits eventually will also include business associates, both business associates and covered entities should prepare now for the prospect of a HIPAA audit. Some suggested steps include:

- Since audited entities must provide documentation of HIPAA privacy and security compliance within only 10 days, these materials should be readily available, up-to-date, accurate, and in full compliance with all applicable requirements. These include up-to-date policies and procedures and business associate agreements; documentation of HIPAA Security Rule compliance, including documentation of all risk assessments and implementation of appropriate safeguards that address all of the Security Rule standards; documentation of investigation and mitigation of all reported breaches; documentation of compliance with breach notification requirements; and documentation of employee training.
- Covered entities and business associates should prepare for OCR's site visits by ensuring that all written policies and procedures are fully implemented as drafted. A HIPAA compliance program that is robust on paper, but that is not fully operational "on the ground," will not suffice. All employees should understand the rules applicable to their job responsibilities, be able to identify the privacy and security officers, and know how to report suspected problems.
- Covered entities and business associates should closely monitor the OCR web site for audit-related announcements. OCR stated that it will, "broadly share best practices gleaned though the audit process and guidance targeted to observed compliance challenges via," its web site and other outreach portals.
- A team should be assigned to handle audit readiness. A prepared team also should be in place to respond to an audit should one be initiated.
- Covered entities and business associates should conduct an internal audit of HIPAA policies and procedures now to evaluate the level of current compliance and fill in any missing gaps before the auditors come knocking.

Conclusion

The new audit program launched by the Department of Health and Human Services' Office for Civil Rights is a continuation of the increased HIPAA enforcement trend that has emerged over the last few years. OCR has shown a new willingness not only to impose financial penalties for non-compliance more often, but also to impose very large monetary penalties and to pursue smaller organizations. Of the nine cases in which OCR has imposed monetary penalties, five involved fines of $1 million or more.

OCR also announced last month that it has entered a $100,000 settlement with a five physician cardiology practice. Leon Rodriguez, director of OCR, stated, "We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity." Given this sentiment and in light of OCR's current audit activity, covered entities and business associates of any size that have neglected to implement a robust HIPAA compliance program or that have been lax about HIPAA should improve their level of compliance without delay.