Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Preparing For HIPAA's New Audit Program

Law360, New York (December 19, 2011, 12:32 PM ET) -- As required by the 2009 Health Information Technology for Economic and Clinical Health Act, the U.S. Department of Health and Human Services has announced the rollout of a new audit initiative to assess compliance across the nation with the privacy and security standards for protected health information under the Health Insurance Portability and Accountability Act of 1996, including the breach notification rules in the HITECH Act.

All "covered entities" under HIPAA — including health care providers and group health plans of all sizes — must take notice of this development in HIPAA enforcement and take immediate steps in preparation for the possibility of an audit as well as the possibility of penalties for serious failures to implement the required compliance protocols.

Background

Ever since implementation of the HIPAA privacy and security standards first began in 2003, covered entities have been required to establish and maintain a variety of compliance mechanisms, including written policies and procedures, training of responsible workforce members, business associate agreements, relevant notices to patients or plan participants, and health plan document amendments. More recently, covered entities have had to implement procedures to comply with the notification requirements under the HITECH Act relating to certain breaches of the privacy or security of individuals' protected health information.

Until now, most compliance actions have been complaint-driven investigations arising from alleged violations of the HIPAA privacy or security standards. In some cases — particularly in egregious cases involving the theft or sale of protected health information, or the failure of a covered entity to cooperate with an investigation — substantial civil monetary and criminal penalties have been imposed.

Note that the HITECH Act increased the potential penalties for violations of the HIPAA privacy and security standards. For example, the maximum total civil monetary penalty that may be imposed on a covered entity for all violations of an identical requirement or prohibition during a calendar year has increased from $25,000 to $1.5 million.

HITECH and the New Audit Program

Pursuant to the HITECH Act, this month HHS begins a more robust enforcement program under HIPAA by auditing a range of covered entities for compliance. Indications by HHS are that for now the audits are primarily "compliance improvement activities." Accordingly, the audit program appears to be intended to assess and improve the current state of compliance by covered entities, rather than to penalize covered entities for the failure to abide by the regulations. However, the imposition of fines by HHS for noncompliance always remains a possibility, especially for serious compliance issues.

Complete information about the new audit program, including anticipated timelines and on-site visits, may be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. According to HHS, the pilot audit program includes a limited number of audits that began in November and will be completed by the end of December 2012. The results of the initial audits will determine how the rest of the audits will be conducted. Any covered entity is eligible for an audit (business associates will be included in future audits).

Covered entities will be selected in this first round of audits "to provide a broad assessment of a complex and diverse health care industry." The audits will accordingly cover as wide a range of types and sizes of covered entities as possible. HHS has also stressed that covered entities will be expected to cooperate fully with the audits, per the relevant requirements of the regulations In general, the audits will begin when covered entities that are selected for an audit are notified in writing and asked to provide documentation of their privacy and security compliance efforts.

Covered entities will be expected to provide requested documents within ten days of such requests. Audits will also include a site visit, which will begin between 30 to 90 days after notice is provided. On-site visits could last between three to 10 business days and will include observations of operations and interviews with responsible members of the covered entity's workforce.

The auditor's report will be submitted to the HHS Office for Civil Rights after the covered entity has had an opportunity to review the report and provide written comments to the auditor. The covered entity will also have the opportunity to discuss compliance issues identified in the report and to describe corrective actions implemented to address such concerns before the final report is submitted. The auditor's final report will incorporate the steps the covered entity has taken to resolve any compliance issues identified by the audit and will describe any best practices of the covered entity.

Recommendations and Next Steps

In light of the new audit program, covered entities should perform a self-audit with the assistance of experienced consultants to identify gaps in compliance that may have always existed or may have developed over time. Given recent changes in the law, especially the new breach notification rules, covered entities should confirm that their policies and procedures and business associate agreements are complete and up-to-date. Swift action should be taken to remedy any shortcomings that may be revealed by self-audit.

Covered entities should also be prepared to respond to requests for documentation within the required 10-day period. For example, the privacy standards require that covered entities document certain elements of their privacy compliance plans (e.g., policies and procedures, privacy notices, business associate contracts, personnel designations, training, complaints, disposition of complaints, and workforce member sanctions). Covered entities should maintain a list of such elements, including the location of the required documentation.

If nothing else, covered entities of all sizes need to know that a new day in enforcement is here. HIPAA privacy and security compliance will have to be a greater priority than ever before for most covered entities.

--By Mark C. Lewis and Andrew Elbon, Bradley Arant Boult Cummings LLP

Mark Lewis and Andrew Elbon are partners in the Nashville, Tenn., office of Bradley Arant Boult Cummings.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.