Benefits & Health Care Alert

Published by Bradley Arant Boult Cummings LLP

New Audit Program for HIPAA Privacy & Security Compliance Changes Enforcement Landscape for Covered Entities

November 30, 2011

Authors

Mark C. Lewis
615.252.2347
mlewis@babc.com

Andrew Elbon
615.252.2378
aelbon@babc.com

As required by the HITECH Act, the U.S. Department of Health and Human Services ("HHS") 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 ("HIPAA"), including the breach notification rules in the HITECH Act. All "covered entities" under HIPAA—including healthcare 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 $1,500,000.

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 non-compliance always remains a possibility, especially for serious compliance issues.

Complete information about the new audit program, including anticipated timelines and onsite visits, may be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. According to HHS, the pilot audit program will include a limited number of audits to begin this month and to 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. Onsite visits could last between three to ten 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 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 ten-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.

If you have any questions about the new HHS audit program, please contact Andrew Elbon, Mark Lewis, or any other attorney in the Employee Benefits & Executive Compensation Group or the Health Care Group at Bradley Arant Boult Cummings LLP.

BRADLEY ARANT BOULT CUMMINGS LLP OFFICE LOCATIONS:

ALABAMA
One Federal Place
1819 Fifth Avenue North
Birmingham, AL 35203-2119
205.521.8000

200 Clinton Avenue West, Suite 900
Huntsville, AL 35801-4900
256.517.5100

Alabama Center for Commerce
401 Adams Avenue, Suite 780
Montgomery, AL 36104
334.956.7700

MISSISSIPPI
188 E. Capitol Street, Suite 400
Jackson, MS 39201
601.948.8000

NORTH CAROLINA
100 North Tryon Street, Suite 2690
Charlotte, NC 28202
704.332.8842

TENNESSEE
1600 Division Street, Suite 700
Nashville, TN 37203
615.244.2582

WASHINGTON, DC
1615 L Street, N.W.
Suite 1350
Washington, DC 20036
202.393.7150