Published on *The National Law Review* https://natlawreview.com

HIPAA Privacy and Security Audit Program Begins This Month

Article By:

W. Reece Hirsch

Andy R. Anderson

HIPAA-covered entities, including employer health plan sponsors, should watch the mail for a letter from the Office for Civil Rights (OCR).

The **Health Information Technology for Economic and Clinical Health (HITECH) Act** requires the **Department of Health and Human Services** to conduct periodic audits of covered entities and business associates to ensure compliance with the **HIPAA** privacy and security rules and breach notification standards. Beginning this month and running through 2012, OCR's new pilot program will audit 150 covered entities.

OCR's independent third-party auditor will select a wide variety of covered entities for audit during the pilot program. Selected covered entities will have 10 days to provide documentation of their HIPAA privacy and security compliance after they receive notification.

During the pilot program, every audit will include a site visit during which auditors will interview key personnel and observe processes and operations to help determine compliance. Covered entities should expect between 30 and 90 days' notice prior to a site visit, which will last between 3 and 10 business days, depending upon the complexity of the covered entity and the access given to materials and staff.

Following the site visit, the auditor will provide the covered entity with a draft report, and the covered entity will have 10 business days to provide written comments back to the auditor. The auditor will then submit a final audit report to OCR.

OCR has presented the audit pilot program as a "compliance improvement activity" aimed at enabling OCR to better understand compliance efforts, additional types of technical assistance that would be useful, and the effectiveness of various corrective actions. However, covered entities should be mindful that if an audit reveals a serious compliance issue, OCR may initiate a compliance review to address the problem.

Covered entities should consider conducting a "self-audit" before OCR comes

knocking to ensure the following:

- Business associate agreements are up to date
- Current HIPAA privacy and security documents, procedures, and notices are in place
- Individuals who handle protected health information are trained, and their training is documented

National Law Review, Volume I, Number 324