

HIPAA Update

Long-Awaited Phase 2 HIPAA Audits Now Begin

In an effort to improve industry awareness of compliance obligations under the Health Insurance Portability and Accountability Act ("HIPAA") Privacy, Security and Breach Notification Rules, the Office for Civil Rights at the U.S. Department of Health and Human Services ("OCR") announced Monday that it is beginning Phase 2 of audits for covered entities and business associates. The much anticipated 2016 Phase 2 HIPAA Audit Program will consist of both desk and on-site audits. It will include a review of the policies and procedures developed, implemented and used by covered entities and their business associates to determine conformity with the Privacy, Security and Breach Notification Rules.

Background

The 2016 Phase 2 HIPAA Audit Program follows the pilot audit program implemented by the OCR in 2011 and 2012. The pilot program was designed to review and assess the controls and processes of 115 covered entities. Having completed its comprehensive assessment of the pilot program's efficacy and compiled the results of the audits, the OCR is now turning its attention to covered entities *and* their business associates.

Audit Procedure

All covered entities and business associates are eligible for the 2016 Phase 2 HIPAA Audit Program. The OCR is currently obtaining and verifying contact information of covered entities and business associates. Once contact information is collected, the OCR will send a questionnaire to

covered entities and business associates to gather data about their size, type and operations in an effort to create a pool of covered entities and business associates representing a wide range of health care providers, health plans, health care clearinghouses and business associates. An organization that does not respond to the OCR's request for address verification or questionnaire can still be selected for an audit or subjected to a compliance review. Organizations that have an open complaint investigation or that are currently undergoing a compliance review will not be audited.

The audit process will consist of three phases, including desk audits and onsite audits of covered entities and business associates. The first round of desk audits will be for covered entities and the second round for business associates. OCR will send an email to organizations selected for audit and the organization will have 10 business days to submit requested information.

On-site audits will be more comprehensive than desk audits and are expected to take between three to five days.

Following each audit, the OCR will review and analyze the information obtained to prepare final reports. Organizations will be given an opportunity to respond to the audit findings. In the event an audit report reveals a serious compliance issue, the OCR may initiate a compliance review to further investigate the entity. Investigation can result in the imposition of financial penalties.

Preparing for Phase 2

Here is how you can prepare for Phase 2.

- Review your organization's compliance program, including HIPAA policies and procedures.
- Watch for correspondence from OCR and ensure that emails from OCR are not being trapped in your spam or junk folder.
- Review the Phase 1 Audit Protocol.
- Conduct a mock audit, assuming the role of an auditor and review your organization's documentation from the perspective of an auditor.
- Perform a detailed risk assessment.

- Compile a list of Business Associates.
- Educate and train employees about HIPAA privacy and security rules and compliance.

An OCR HIPAA audit can be an overwhelming, complex and confusing experience for covered entities and business associates, especially considering a possible compliance review and potential financial penalties. Aronberg Goldgehn can assist covered entities and business associates in preparing for and navigating the HIPAA audit process.

If you have any questions about this Update, please contact [Paul A. Gilman](#), [Lindsay P. Lollo](#) or [Mitchell J. Melamed](#) or the Aronberg Goldgehn attorney with whom you normally consult.