

WHAT YOU NEED TO KNOW



HIPAA Phase 1 Audits

The Health Insurance Portability and Accountability Act (HIPAA) established national standards to secure and protect the privacy of health information. The Health Information Technology for Economic and Clinical Health Act (HITECH) requires the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) to conduct audits of covered entities and business associates in order to ensure compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

OCR initiated a [pilot program](#) in 2012 to assess the processes implemented by 115 covered entities to comply with HIPAA's requirements. The pilot program was a three-step process: (1) initial protocol development, (2) test of these protocols by conducting 20 audits, and (3) full audit execution using revised protocol materials, which were completed by the end of December 2012.

OCR selected a pool of covered entities for audits that broadly represented a wide range of healthcare providers, health plans, and healthcare clearinghouses. Criteria to select entities to be audited included whether the entity was public or private, size of the entity, affiliation with other healthcare organizations, the type of entity and relationship to patient care, past and present interaction with OCR concerning HIPAA enforcement and breach notification, as well as geographic factors.

A wide range of covered entities were audited in Phase 1. The audit process began when selected entities received a notification letter from OCR notifying them of their selection and asking them to provide documentation of their privacy and security compliance efforts. Every audit included a site visit during which auditors interviewed key personnel and observed processes to determine compliance. Following the site visit, auditors developed a draft audit report which described how the audit was conducted, what the findings were, and what actions the covered entity took in response to those findings. The covered entity had the opportunity to remedy any compliance issues. The final report included the steps the entity took to resolve any compliance issues identified by the audit and it also described best practices.

OCR used the final audit to understand HIPAA compliance efforts and to determine the types of technical assistance that should be developed and the types of corrective action that are most effective. The technical assistance and best practices that OCR generated assisted covered entities and business associates in improving their efforts to keep health records safe and secure.

7/28/2016

UBA Compliance Advisor

This information is general and is provided for educational purposes only. It is not intended to provide legal advice.
You should not act on this information without consulting legal counsel or other knowledgeable advisors.



Shared Wisdom. Powerful Results.®