

OCR HIPAA Audit Response Plan

General

Background

The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, require HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards. To implement this mandate, OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance. Audits conducted during the pilot phase started in November 2011 and will conclude by December 2012.

Department of Health and Human Services / Office of Civil Rights Audit Process

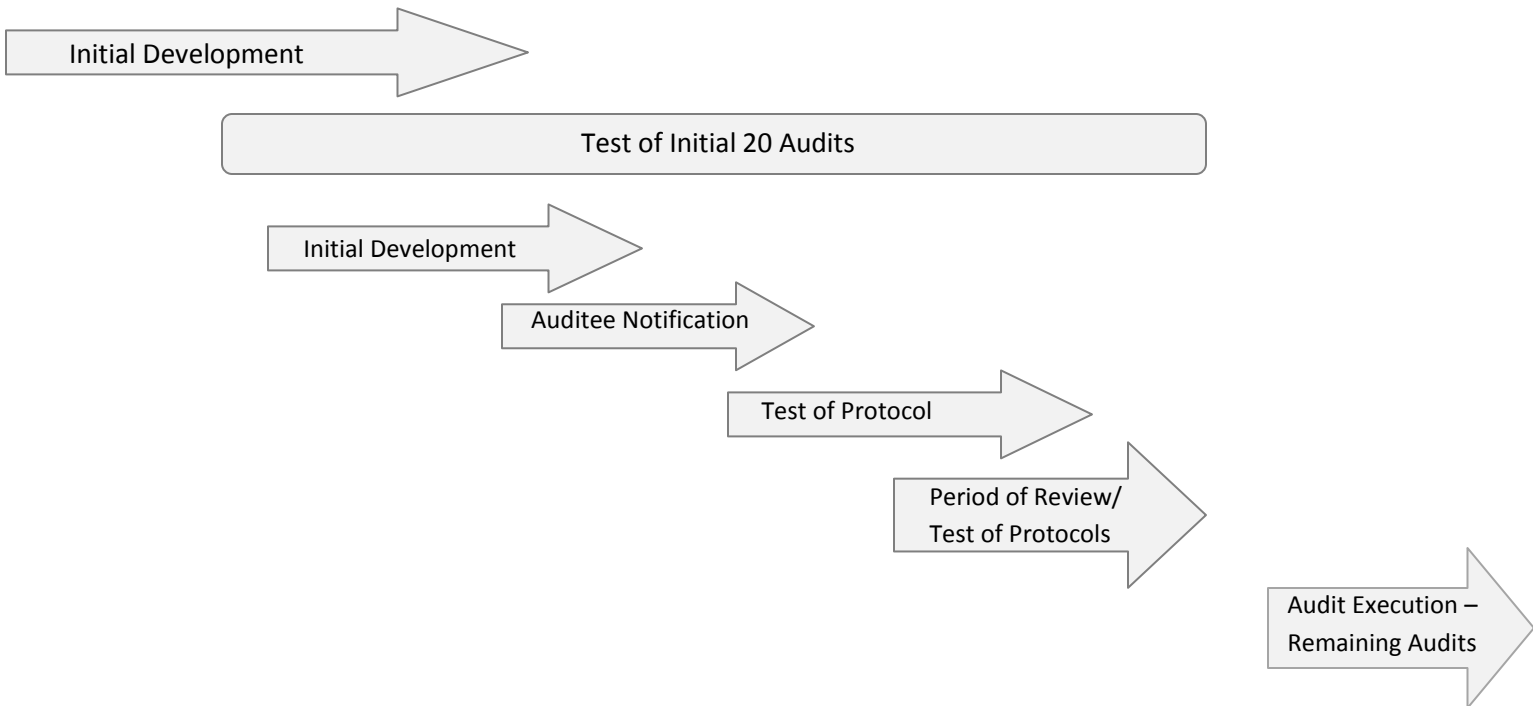
The Department of Health and Human Services (HHS) /Office of Civil Rights (OCR) has been charged with conducting approximately 150 audits of covered entities and business associates as part of the HIPAA/HITECH enforcement efforts. Details of the audit program are available on the HHS website at the following URL: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html>

HHS/OCR has contracted with a consulting company (KPMG) who will be performing the audits. Although detailed information on what they will audit has not been officially released, other than HIPAA compliance, there is some information available. The available information has been summarized in the following sections.

When Will Audits Begin?

According to recent reports HHS/OCR has notified 5 of the first 20 organizations to be audited in 2011. Notification for the remaining 15 organizations to be audited in the first phase is pending. These audits are being used as a test phase to evaluate the audit protocols. The remaining 130 organizations will be audited between April and December of 2012.

The figure below is provided by OCR and outlines their timeline for completing the audits. Based on this information if an organization isn't notified by December 15th then they have until April of 2012 before the next round of notifications.



How will the Federal Government conduct the audit?

The privacy and security performance audit process will include generally familiar audit mechanisms. Entities selected for an audit will be informed by OCR of their selection and asked to provide documentation of their privacy and security compliance efforts. In this pilot phase, every audit will include a site visit and result in an audit report.

During site visits, auditors will interview key personnel and observe processes and operations to help determine compliance. Following the site visit, auditors will develop and share with the entity a draft report; audit reports generally describe how the audit was conducted, what the findings were and what actions the covered entity is taking in response to those findings.

Prior to finalizing the report, the covered entity will have the opportunity to discuss concerns and describe corrective actions implemented to address concerns identified. The final report submitted to OCR will incorporate the steps the entity has taken to resolve any compliance issues identified by the audit, as well as describe any best practices of the entity.

What is the General Timeline for an Audit?

When a covered entity is selected for an audit, OCR will notify the covered entity in writing. The OCR notification letter will introduce the audit contractor, explain the audit process and expectations in more detail, and describe initial document and information requests. It will also specify how and when to return the requested information to the auditor. OCR expects covered entities and business associates who are the subject of the audit to provide requested information within 10 business days of the request for information.

OCR expects to notify selected covered entities between 30 and 90 days prior to the anticipated onsite visit. Onsite visits may take between 3 and 10 business days depending upon the complexity of the organization and the auditor's need to access materials and staff. After fieldwork is completed, the auditor will provide the covered entity with a draft final report; a covered entity will have 10 business days to review and provide written comments back to the auditor. The auditor will complete a final audit report within 30 business days after the covered entity's response and submit it to OCR.

What to expect during the audit?

Guidance from HHS/OCR on what they will be auditing has not been detailed or specific. Besides a general approach of focusing on the HIPAA & HITECH regulations there are two sources which identify specific information requests. The first source is a document published by Dept of Health & Human Services and posted on their website. It has since been removed and is not available from official sources.

The second list of requirements came from Piedmont after their audit by OCR. Both sources are similar in content and it should be noted that OCR may request different information from the organizations being audited.

OCR Sample Interview and Document Request

1. Personnel that may be interviewed
 - a. President, CEO or Director
 - b. HIPAA Compliance Officer
 - c. Lead Systems Manager or Director
 - d. Systems Security Officer
 - e. Lead Network Engineer and/or individuals responsible for:
 - i. administration of systems which store, transmit, or access Electronic Protected Health Information (EPHI)
 - ii. administration systems networks (wired and wireless)
 - iii. monitoring of systems which store, transmit, or access EPHI
 - iv. monitoring systems networks (if different from above)
 - f. Computer Hardware Specialist
 - g. Disaster Recovery Specialist or person in charge of data backup
 - h. Facility Access Control Coordinator (physical security)

- i. Human Resources Representative
 - j. Director of Training
 - k. Incident Response Team Leader
 - l. Others as identified....
2. Documents and other information that may be requested for investigations/reviews
- a. Policies and Procedures and other Evidence that Address the following:
 - Prevention, detection, containment, and correction of security violations
 - Employee background checks and confidentiality agreements
 - Establishing user access for new and existing employees
 - List of authentication methods used to identify users authorized to access EPHI
 - List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
 - List of software used to manage and control access to the Internet
 - Detecting, reporting, and responding to security incidents (if not in the security plan)
 - Physical security
 - Encryption and decryption of EPHI
 - Mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives)
 - Monitoring systems use - authorized and unauthorized
 - Use of wireless networks
 - Granting, approving, and monitoring systems access (for example, by level, role, and job function)
 - Sanctions for workforce members in violation of policies and procedures governing EPHI access or use
 - Termination of systems access
 - Session termination policies and procedures for inactive computer systems
 - Policies and procedures for emergency access to electronic information systems
 - Password management policies and procedures
 - Secure workstation use (documentation of specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage)
 - Disposal of media and devices containing EPHI