

[Skip Navigation](#)

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

OCR HIPAA Audit Program

Overview: The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, requires 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 will begin November 2011 and conclude by December 2012.

Program Objectives: The audit program serves as a new part of OCR's health information privacy and security compliance program. OCR will use the audit program to assess HIPAA compliance efforts by a range of covered entities. Audits present a new opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews. OCR will broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges via this web site and other outreach portals.

When Will Audits Begin?

The pilot audit program is a three step process. The first step entailed developing the audit protocols. Next, a limited number of audits will be conducted in an initial wave to test these protocols. OCR expects the initial audits to begin in November 2011. The results of the initial audits will inform how the rest of the audits will be conducted. The last step will include conducting the full range of audits using revised protocol materials. All audits in this pilot will be completed by the end of December, 2012.

Related Links:

[Initial Notification Letter Sample](#)
[HITECH Act authority For Covered Entities](#)
[Government Auditing Standards](#)

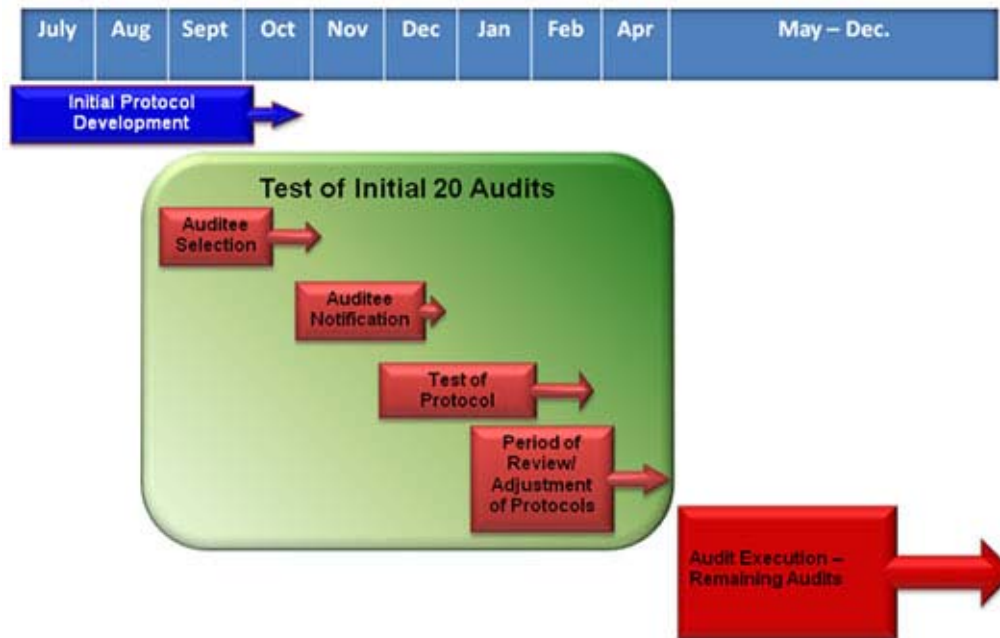
[HHS Home](#) | [Questions?](#) | [Contacting HHS](#) | [Accessibility](#) | [Privacy Policy](#) | [FOIA](#) | [Disclaimers](#) | [Inspector General](#) | [No FEAR Act](#) | [Viewers & Players](#)
[The White House](#) | [USA.gov](#) | [HHS Archive](#) | [Pandemic Flu](#)

U.S. Department of Health & Human Services · 200 Independence Avenue, S.W. · Washington, D.C. 20201

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy



Who Will Be Audited?

Every covered entity and business associate is eligible for an audit. Selections in the initial round will be designed to provide a broad assessment of a complex and diverse health care industry. OCR is responsible for selection of the entities that will be audited. OCR will audit as wide a range of types and sizes of covered entities as possible; covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses may all be considered for an audit. We expect covered entities to provide the auditors their full cooperation and support and remind them of their cooperation obligations under the HIPAA Enforcement Rule.

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Business Associates will be included in future audits.

How Will the Audit Program Work?

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.

[HHS Home](#) | [Questions?](#) | [Contacting HHS](#) | [Accessibility](#) | [Privacy Policy](#) | [FOIA](#) | [Disclaimers](#) | [Inspector General](#) | [No FEAR Act](#) | [Viewers & Players](#)
[The White House](#) | [USA.gov](#) | [HHS Archive](#) | [Pandemic Flu](#)

U.S. Department of Health & Human Services · 200 Independence Avenue, S.W. · Washington, D.C. 20201

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy



References to days are in business days.

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

[HHS Home](#) | [Questions?](#) | [Contacting HHS](#) | [Accessibility](#) | [Privacy Policy](#) | [FOIA](#) | [Disclaimers](#) | [Inspector General](#) | [No FEAR Act](#) | [Viewers & Players](#)
[The White House](#) | [USA.gov](#) | [HHS Archive](#) | [Pandemic Flu](#)

U.S. Department of Health & Human Services · 200 Independence Avenue, S.W. · Washington, D.C. 20201

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

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 Happens After an Audit?

Audits are primarily a compliance improvement activity. OCR will review the final reports, including the findings and actions taken by the audited entity to address findings. The aggregated results of the audits will enable OCR to better understand compliance efforts with particular aspects of the HIPAA Rules. Generally, OCR will use the audit reports to determine what types of technical assistance should be developed, and what types of corrective action are most effective. Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to address the problem. OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

How will Consumers Be Affected?

The audit program represents one more avenue by which OCR ensures compliance with HIPAA protections of health information to the benefit of consumers. For example, the audit program may uncover reasons many health information breaches are occurring and help OCR create tools for covered entities to better protect individually identifiable health information. Concerns about compliance identified and corrected by an audit will serve to improve the privacy and security of health records. The technical assistance and best practices that OCR generates will also assist covered entities and business associates in improving their efforts to keep health records safe and secure. OCR continues to accept complaints from individuals and covered entities continue to have the obligation to accept complaints from persons about their HIPAA Rule activities.

[HHS Home](#) | [Questions?](#) | [Contacting HHS](#) | [Accessibility](#) | [Privacy Policy](#) | [FOIA](#) | [Disclaimers](#) | [Inspector General](#) | [No FEAR Act](#) | [Viewers & Players](#)
[The White House](#) | [USA.gov](#) | [HHS Archive](#) | [Pandemic Flu](#)

U.S. Department of Health & Human Services · 200 Independence Avenue, S.W. · Washington, D.C. 20201



DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF THE SECRETARY

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
<http://www.hhs.gov/ocr>

Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

Date

Name of Entity

Address of Entity

Point of Contact of Entity

Dear Covered Entity:

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (45 CFR Part 160 and Part 164 Subparts C and E). These rules are designed to provide important health information privacy and security protections and rights for individuals. The OCR is committed to developing and enforcing strong health information privacy protections that do not impede access to quality health care.

The American Recovery and Reinvestment Act of 2009 (ARRA) requires HHS to audit covered entity and business associate compliance with the HIPAA privacy and security standards. To effectively implement this statutory mandate, OCR has engaged the services of a professional public accounting firm (KPMG LLP) to conduct performance audits, using generally accepted government auditing standards. You are receiving this letter because OCR has selected [Name of entity] to be the subject of an audit.

These audits are a new facet of the OCR health information privacy and security compliance program. Audits present an opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's established complaint investigations and compliance reviews. OCR will broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges. OCR will assess whether to open a separate compliance review in cases where an audit indicates serious compliance issues.

Request for Information and Points of Contact

In the attached letter, KPMG LLP requests certain information be provided by you in order to facilitate the audit process. Additionally, they provide contact information for the audit firm personnel responsible for conducting the audit. Please recognize that KPMG LLP is requesting and reviewing these documents solely as a contractor to OCR and on its behalf and pursuant to its audit authority. This letter serves to notify you that the audit shall begin within the next 30 to 90 calendar days from the date of this letter. The results of the audit firm's work, including your management's written response to any reportable findings will be presented in a final report to OCR.

We expect you to provide KPMG LLP your full cooperation and support and remind you of your cooperation obligations under the HIPAA Enforcement Rule.

Sincerely,

Leon Rodriguez
Director
Office for Civil Rights, DHHS