HIPAA audits

The Department of Health and Human Services' Office for Civil Rights (OCR) conducts periodic audits to ensure that covered entities and their business associates comply with the requirements of HIPAA's regulations. In 2001, OCR established a pilot audit program in which it measured the efforts of covered entities through a set of instructions known as an audit program protocol. The protocol was updated in 2016.

Half the dues, all the AMA benefits!

- Free access to JAMA Network™ and CME
- Save hundreds on insurance
- Fight for physicians and patient rights

Join for Half Dues

In 2016, OCR updated this protocol for the second phase of its HIPAA Audit Program. This phase of the audit program involves the review of policies and procedures by covered entities and their business associates to meet the requirements of HIPAA's Privacy, Security and Breach Notification Rules.

- HIPAA Privacy Rule
- HIPAA Security Rule & Risk Analysis
- HIPAA Breach Notification Rule

Who is audited

Every covered entity and business associate is eligible for an audit.

The selection process

A questionnaire designed to gather data about the size, type and operations of potential auditees will be sent to covered entities and business associates. As a part of the preaudit screening questionnaire, OCR is asking that entities identify their business associates.

If a covered entity or business associate fails to respond to information requests, OCR will use publically available information about the entity to create its audit pool. An entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

The audit program

OCR plans to conduct desk and onsite audits. Entities selected for an audit will be sent an email notification of their selection and will be asked to provide documents and other data in response to a document-request letter. The OCR notification letter will introduce the audit team, explain the audit process and discuss OCR's expectations in more detail. In addition, the letter will include initial requests for documentation.

OCR expects covered entities being audited to submit requested information via OCR's secure portal within 10 business days of the date on the information request. Audited entities will submit documents online via a secure audit portal on OCR's website. Auditors will then review the documentation submitted and develop and share draft findings with the entity. Auditees will have the opportunity to respond to these draft findings; their written responses will be included in the final audit report.

- AMA EdHub™: The nuts and bolts of achieving HIPAA Security Rule compliance through effective risk assessment
- U.S. Department of Health & Human Services (HHS) privacy and security toolkit
- Understanding patients' health information rights (PDF)
- HIPAA privacy and security toolkit: Helping your practice meet compliance requirements (PDF)

This resource is provided for informational and reference purposes only and should not be construed as the legal advice of the American Medical Association. Specific legal questions regarding this information should be addressed by one's own counsel.