

# LEGISLATIVE BRIEF

Brought to you by Midlands Financial Benefits, Inc.

## HHS Launches HIPAA Audit Program

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, the Department of Health and Human Services (HHS), Office of Civil Rights (OCR) has announced a pilot audit program.

Beginning in **November 2011**, an initial 20 audits will be conducted to establish and test audit protocol. The results of the initial audits will determine how the rest of the audits will be conducted. The remaining audits, about 150 in all, will be conducted over the next year using revised protocol materials. The pilot will be completed by the **end of December 2012**.

This Midlands Financial Benefits, Inc. Legislative Brief provides an overview of the HIPAA Audit Program.

### WHAT IS THE GOAL OF THE AUDIT PROGRAM?

The audits are intended to assess HIPAA compliance efforts and improve compliance with health information privacy and security requirements. OCR will use the audit reports to:

- Determine what types of technical assistance and tools should be developed to assist covered entities in improving their efforts to keep health records safe and secure;
- Discover risks and vulnerabilities; and
- Realize what types of corrective actions are most effective.

### WHO MAY BE AUDITED?

Every covered entity and business associate is subject to being selected for an audit. However, the initial round of audits will be of covered entities only.

OCR will audit as many different types and sizes of covered entities as possible. The initial 20 covered entities to be audited will include covered individual and organizational providers of health services, health plans of all sizes and functions and health care clearinghouses.

### WHAT IS THE PROCESS FOR THE AUDIT?

Covered entities chosen for an audit will be notified in writing by OCR. The written notification will explain the program and request documentation of the privacy and security compliance efforts of the covered entity. The covered entity will have up to 10 business days to provide the requested documentation.

Selected covered entities can expect an onsite visit between 30 and 90 days after notification. Onsite visits may take between three and 10 business days depending upon the complexity of the organization as well as the quantity of materials and number of staff the auditor needs to access.



# HHS Launches HIPAA Audit Program

---

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.

OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

## **WHAT ACTION STEPS SHOULD COVERED ENTITIES AND BUSINESS ASSOCIATES BE TAKING NOW?**

Covered entities and business associates should review their compliance with HIPAA requirements to determine if any changes should be made in light of the possibility of being selected for audit. The review may include:

- Reviewing and updating written HIPAA policies and procedures, as necessary, for privacy and security rules and breach notification requirements;
- Reviewing and updating notices to individuals, including revising model notices as necessary;
- Ensuring that employees with access to protected health information have received the necessary HIPAA training;
- Reviewing and updating business associate agreements; and
- Verifying that privacy and security rules in the written documents are being put into practice. If they are not, and the current practices are HIPAA compliant, the documents should be revised to reflect current practice.

## **ADDITIONAL GUIDANCE**

More information on the audit program is available from OCR at:  
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html>.

This Midlands Financial Benefits, Inc. Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

© 2011 Zywave, Inc. All rights reserved.

KP 11/11