United Actuarial Services, Inc.
Actuaries and Consultants

2011-74

November 11, 2011

CLIENT BULLETIN

OCR HIPAA Privacy and Security Rules Audit Program

Up to 150 Audits To Be Performed Between November 2011 and December 2012

The *American Recovery and Reinvestment Act of 2009 (ARRA),* in Section 13411 of the *HITECH Act*, requires the Department of Health and Human Services (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 agency charged with enforcement – the Office of Civil Rights (OCR) – announced it is setting up a pilot program to perform up to 150 audits of covered entities to assess privacy and security compliance between November 2011 and December 2012. A multiemployer health plan is generally a "covered entity."

The following questions and answers as well as additional information on the audit program can be found on the OCR website at: *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.*

When Will Audits Begin?
A limited number of audits (about 20) will be conducted in an initial wave beginning in November 2011.

Who Will Be Audited?
Every covered entity and business associate is a possible candidate for an audit. However, selections in the initial round will be focus on the health care industry. Business Associates will be included in future rounds of 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

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: mewing@unitedactuarial.com

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 an 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; and the 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 receiving 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 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 <u>not</u> post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

Now would be a good time to review your privacy and security procedures and to contact your Fund Professionals with any questions or concerns that you have.

*   *   *

LEGAL DISCLAIMER: Information contained in this publication is not legal advice, and should not be construed as legal advice. If you need legal advice upon which you can rely, you should seek a legal opinion from your attorney.