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.

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.

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

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: http://www.purdue.edu/hipaa or contact: Joan Vaughan, Director, HIPAA Privacy Compliance, x61927
FAQ’s of the Month

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 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.

Standards for Wireless Communications... continued

Wireless networking, especially in medical facilities is becoming more and more prevalent. There are some important issues to be taken into consideration before implementing a wireless network or using wireless technology for transmitting confidential data or data protected by law. The ITaP Networks and Security group should be contacted for recommendation on how to best safeguard the data on a wireless network or for appropriate alternatives, prior to implementing a solution.

Initially, the classification of data to be transmitted needs to be determined, http://www.purdue.edu/securePurdue/policies/dataConfident/restrictions.cfm.

Yes. The HIPAA Privacy Rule explicitly defines organizations that accredit covered entities as business associates. See the definition of “business associate” at 45 CFR 160.103.

Like other business associates, accreditation organizations provide a service to the covered entity which requires the sharing of protected health information. The business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, covered entities may disclose a limited data set of protected health information, not including direct identifiers, to an accreditation organization, subject to a data use agreement. See 45 CFR 164.514(e).

If only a limited data set of protected health information is disclosed, the satisfactory assurances required of the business associate are satisfied by the data use agreement.

Standards for Wireless Communications... continued

Purdue has published data handling guidelines that address proper safeguards for storage and transmission of data, determined by its classification public, sensitive or restricted, http://www.purdue.edu/securePurdue/procedures/dataHandling1.cfm.

If there is a significant reason that the data needs to be transmitted using wireless communications and the data guidelines prohibit this method of transmission, an exception procedure must be followed and an exception request submitted to ITaP Networks Security, http://www.purdue.edu/securepurdue/bestpractices/deviationProcedure.cfm. ITaP will review the request and will either approve, deny or suggest alternative implementation solutions.

If it is determined that wireless communications will be used, the Wireless Network Acceptable Use Standard should be used and followed http://www.purdue.edu/securepurdue/bestPractices/wirelessUseStandards.cfm. Also, refer to the Mobile Device Security Best Practices for information related to safeguarding of mobile devices where protected data will be transmitted and stored. http://www.purdue.edu/securepurdue/bestpractices/mobileDevice.cfm.