Included in this newsletter is guidance on various HIPAA-related topics that impact your everyday work life. Hopefully, it will help answer some of your questions about how HIPAA relates to your work processes.

HIPAA Privacy & Security Audit Program

Derived from an article provided by the Office for Civil Rights

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 piloted a program to perform 115 audits of covered entities to assess privacy and security compliance. Audits conducted during the pilot phase began November 2011 and concluded in December 2012.

Audit Pilot Program

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.

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 (continued page 2)

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 telephone: (765) 496-1927 e-mail: jvaughan@purdue.edu
As we roam the Internet researching things, liking things or purchasing things, we create a digital profile. It isn’t something we intentionally create, but Internet marketers track us and create a data profile of our habits, likes, hobbies, and political leanings. They want to help us find the items or news articles that we have indicated we like by what we visit on the Internet. When you log into Facebook, you will likely notice advertisements that match your interests.

Behavioral tracking is the process of tracking your habits and behaviors online. Online marketers buy information about your online activity to target coupons and campaigns just for you. This can be good but also annoying. There are some guidelines to follow when entering the Internet each day.

- Share the least information on websites. Your email site doesn’t require more than what is needed to receive emails and send them out. Your friends on Facebook probably already have your address and cell phone number. It is better to limit how much you share.

- Log out of Facebook, LinkedIn, online banking or whatever sites you have open that contain your personal information before you surf the Internet. Your searches may be easily tied to whatever else you have open.

Beware of “fan pages.” Sure, you want to like things that your friends post but remember what you post, and like online, doesn’t go away.

Depending on how public you set your profile, many people could see this and maybe that isn’t ok.

Think of your digital profile as an audio recording of everything you say and do. It is a digital record of what you said, what pictures you shared, where you went and with whom, and the location the pictures were taken.

FAQ’s of the Month
Provided by the Office for Civil Rights

Question:
A provider might have a patient's medical record that contains older portions of a medical record that were created by another previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

Answer:
Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

(continued from page 1-Audit Program)

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 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.