



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.

From the Director

There is again a lot of activity within the HIPAA Privacy Compliance Office. The 2009 privacy and security assessments are well underway and several software projects are in process in PUSH and Employee Wellness departments. When software is considered for purchase, the HIPAA compliance director works with ITNS to request information about available security features. Software reviews do not certify that the software meets compliance directives, but attempt to identify minimum capabilities of the software to meet HIPAA security rule requirements if properly configured, and to make configuration recommendations to the staff supporting the software.

In addition, as of 8/1/2009, changes have occurred to the list of covered components. Business Services Computing has reorganized to incorporate OnePurdue support staff and coverage; therefore, includes a larger group of staff. Also, Calumet Business Office for Student Affairs and Calumet Student Service Business Office was covered and Accounts Payable and OnePurdue Initiative are no longer listed.

and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a **breach** of such information. This guidance will be updated annually.

The HHS interim final regulations are effective 30 days after publication in the Federal Register and include a 60-day public comment period.

HITECH Breach Notification Interim Final Rule

Article from the U.S. Department of Health and Human Services

HHS issued regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is **breached**.

These “**breach** notification” regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The regulations, developed by OCR, require health care providers and other HIPAA covered entities to promptly notify affected individuals of a **breach**, as well as the HHS Secretary and the media in cases where a **breach** affects more than 500 individuals. **Breaches** affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of **breaches** at or by the business associate.

“This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care. These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information,” said Robin-sue Frohboese, Acting Director and Principal Deputy Director of OCR.

The regulations were developed after considering public comment received in response to an April 2009 request for information and after close consultation with the Federal Trade Commission (FTC), which has issued companion **breach** notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA.

To determine when information is “unsecured” and notification is required by the HHS and FTC rules, HHS is also issuing in the same document as the regulations an update to its guidance specifying encryption and destruction as the technologies



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



Internet Searches That Put You at Risk

Article from the Secure Purdue News, August 2009

If you search on the web in a popular category, your risks of infection increase.

If you search the web for a song lyric, free music, screen saver or ringtone for your phone, you may be exposing yourself to dangerous content in the sites you visit as well as the items you download. The malware you may come in contact with from these questionable sites and the items you may download from them may compromise your computer and allow malicious individuals and cyber criminals to access personal information such as online banking details.

Searching on the web for popular topics or events increases your risks of compromise. For example, if you checked out the swine flu epidemic, the hackers would have been ready for you. Malicious individuals and cybercriminals are savvy observers of current events that attract large numbers of people. They wait with malware laden sites and files, baiting unsuspecting surfers.

Searching for popular topics like cool ringtones for your phone or “free music downloads” puts you at risk as well. McAfee has analyzed the risk factor for specific search phrases and found that free music downloads put you at risk 20.7 percent of the time. Screensaver searches put you at the highest risk level with 34.4 percent chance of malware infection.

Our best advice when using your computer on the internet is:

- Do Not open email attachments from unknown sources.
- Before opening an unexpected attachment from a known source verify that the known sender actually sent you the attachment.
- Always keep your anti-virus and anti-malware software and definition files up to date.
- Run anti-spyware programs regularly (daily or weekly).
- Set your operating system to always show file extensions so that you know what kind of file you may be downloading or opening.
- Make sure you keep your browser up to date.
- Stick to trusted web sites; some browser add-ons such as Site Advisor, free from McAfee, will let you know if a site is untrusted.
- Other browser add-ons such as NoScript can be used to disallow execution of scripts on all web pages except the ones you trust and allow.

FAQ of the Month

Derived from guidance provided by the Office for Civil Rights



Question:

May a covered entity reuse or dispose of computers or other electronic media that store electronic protected health information?

Answer:

Yes, but only if certain steps have been taken to remove the electronic protected health information (ePHI) stored on the computers or other media before its disposal or reuse, or if the media itself is destroyed before its disposal. The HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of ePHI from electronic media before the media are made available for reuse. See 45 CFR 164.310(d)(2)(i) and (ii). Depending on the circumstances, appropriate methods for removing ePHI from electronic media prior to reuse or disposal may be by clearing (using software or hardware products to overwrite media with non-sensitive data) or purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) the information from the electronic media. If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating, or shredding the media. Covered entities may contract with business associates to perform these services for them.

For more information on proper disposal of ePHI and reuse of electronic media, see the HHS HIPAA Security Series 3: Security Standards – Physical Safeguards. In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.

Internet Searches That Put You at Risk ... Continued

- Never follow a link in an email that wants you to update account/personal information.
- To see the actual URL link location, hold the mouse pointer over a link (usually displays at the bottom of your browser or as screen tip just beneath the link)
- Always make sure that you are on a secure website before entering personal information; https and the pad lock icon in the bottom of your browser indicates you are on a secure website.