Effective March 26, 2013, compliance required by September 23, 2013, Health and Human Services has issued the final rule to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with the goal of strengthening the privacy and security protections for individual’s health information, including genetic information. Following is a summary of the major provisions.

This omnibus final rule is comprised of the following four final rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:
   - Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules’ requirements.
   - Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
   - Expand individuals’ rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
   - Require modifications to, and redistribution of, a covered entity’s notice of privacy practices.
   - Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
   - Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule (referenced immediately below), such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule’s “harm” threshold with a more objective standard and supplants an interim final rule pub-

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
Lock Computers While Away From Workstations

The approved process for leaving your computer powered on while you are away is to use the keystroke combination; Ctrl, Alt, Delete or WIN+L (for Windows machines) and Control+Shift+Eject (for Mac machines). This will lock your computer. This is the most secure process to ensure no one can inadvertently see files you have access to.

WIN 7’s hibernation mode is not secure. By default, it reopens without requiring a password. If you placed your machine in hibernation, it will not securely protect the files open or prevent unauthorized access to data you may have left open. If you want to change the default setting to lock while in sleep mode, go to the Control Panel/System and Security. On the right side of the screen, under Power Options, select the Require a password when the computer wakes. Save this change.

Hibernation is intended as a power saving mode only and by default does not protect access to your files and the programs you may have left open before the machine was put in hibernation status. If you use a laptop, use the same process to securely lock access.

Apple Max OS X users can go to System Preferences, click Security, click the General tab and check the box, Require password to wake this computer from sleep or screensaver. Then, go to System Preferences, click Desktop & Screen saver, click the Screen Saver tab and set a Start screen saver time.

On computers running Linux, the procedure for locking your screen varies by the Linux distribution, so check with the documentation for your version of Linux.

An alternate procedure for all three operating systems is to log out of your computer when you are going to be away for some time.

HHS announces first HIPAA breach settlement involving less than 500 patients

The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services’ (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.

“This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients’ health information,” said OCR Director Leon Rodriguez. “Encryption is an easy method for making lost information unusable, unreadable and undecipherable.”

The Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information, or a “breach,” of 500 individuals or more to the Secretary of HHS and the media within 60 days after the discovery of the breach. Smaller breaches affecting less than 500 individuals must be reported to the Secretary on an annual basis.

A new educational initiative, Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information, has been launched by OCR and the HHS Office of the National Coordinator for Health Information Technology (ONC) that offers health care providers and organizations practical tips on ways to protect their patients’ health information when using mobile devices such as laptops, tablets, and smartphones. For more information, visit www.HealthIT.gov/mobiledevices.

Modifications to HIPAA...continued from page 1

4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

These changes will require a comprehensive review and update of Purdue’s HIPAA policies and procedures, retraining all covered staff, reissuance of business associate agreements and redistribution of the Notice of Privacy Practices. Detailed information will be distributed to affected areas in the coming months.

Purdue University is an equal access/equal opportunity university