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.

Encryption and Physical Security for Laptops and Other Mobile Devices

In a press release, dated September 2, 2015, Health and Human Services announced another significant monetary penalty related to the improper securing of PHI stored on portable media.

Cancer Care Group, P.C. agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). Cancer Care paid $750,000 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Cancer Care Group is a radiation oncology private physician practice, with 13 radiation oncologists serving hospitals and clinics throughout Indiana.

On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured electronic protected health information (ePHI) after a laptop bag was stolen from an employee’s car. The bag contained the employee’s computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients.

OCR’s subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. It had not conducted an enterprise-wide risk analysis when the breach occurred in July 2012. Further, Cancer Care did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice within the organization. OCR found that these two issues, in particular, contributed to the breach, as an enterprise-wide risk analysis could have identified the removal of unencrypted backup media as an area of significant risk to Cancer Care’s ePHI, and a comprehensive device and media control policy could have provided employees with direction in regard to their responsibilities when removing devices containing ePHI from the facility.

“Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients’ health information,” said OCR Director Jocelyn Samuels. “Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information.”

Purdue’s Encryption Procedures for Mobile Devices

Purdue has implemented encryption technologies for all laptops and portable media (such as USB drives and CDs) in HIPAA-covered areas. Guidelines regarding storage of PHI are communicated in the HIPAA training PowerPoint and in the Communication Guidelines.

Information containing PHI should not be removed from the facility unless necessary for limited purposes, such as transfer to a storage facility or to a physician for treatment purposes and approved by the area’s HIPAA Liaison. Paper documents should be stored in a locked trunk of a car and immediately removed upon arrival at the destination. Electronically stored documents must be encrypted when stored or transmitted using the approved encryp-

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, HIPAA Privacy Officer telephone: (765) 496-1927 e-mail: hipaa-privacy@purdue.edu
Consumers increasingly want to communicate electronically with their providers through email or texting. The Security Rule requires that when you send ePHI (electronic Protected Health Information) to your patient, you send it through a secure method and that you have a reasonable belief that it will be delivered to the intended recipient. The Security Rule, however, does not apply to the patient. A patient may send health information to you using email or texting that is not secure. That health information becomes protected by the HIPAA Rules when you receive it.

In this environment of more online access and greater demand by consumers for near real-time communications, you should be careful to use a communication mechanism that allows you to implement the appropriate Security Rule safeguards, such as an email system that encrypts messages or requires patient login, as with a patient portal. If you use an EHR (electronic health record) system that is certified under ONC’s 2014 Certification Rule, your EHR should have the capability of allowing your patients to communicate with your office through the office’s secure patient portal.

Documents containing PHI should NEVER be removed from the facility for “work at home” purposes. Never copy files containing PHI to removable media or a mobile device (such as USB drives, an external hard drive, etc), unless appropriate encryption has been applied and unless there is a compelling business reason that outweighs the risk. For guidance on appropriate encryption solutions contact ITSP via the ITaP help desk x44000.

Devices used to store PHI must have their drives destroyed upon retirement of the device. This may include but is not limited to fax machines, all in one printers, USB drives, computer drives, laptops, computers, CDs, etc.

Laptops must be encrypted. To verify this in Windows 7, go to Start/Control Panel/System and Security/BitLocker Drive Encryption. Depending on the version of operating system, there may not be a System and Security Folder. In that case, BitLocker Drive Encryption may be directly under the Control Panel.

In addition, Purdue’s Chief Information Security Officer has initiated a compliance review of Purdue’s HIPAA covered components’ securing of its mobile devices. HIPAA Liaisons in all covered components are required to immediately coordinate with their IT Support Group to implement encryption technologies for all laptops and portable media (such as USB drives and CDs) in HIPAA-covered areas. The HIPAA Liaison must respond to this requirement stating encryption is in place for your respected area, or outline a plan of action by September 17, 2015.

For further guidance on how to properly secure mobile devices or if you have other HIPAA Security Rule questions, please contact the LuAnn Keyton, HIPAA Risk Analyst, at luann@purdue.edu.