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.

Security Reminders

Derived from information provided by the Centers for Medicare and Medicaid Services

Sharing User IDs

How often have you been tempted to share a system userID and password with another staff member...just for a minute or in a circumstance when it is more convenient or timely not to log out and in under your own ID?

Did you know that the owner of the userID is responsible for every action that takes place under that ID. Actions are logged and activities reviewed. Sharing your ID with someone else is a violation of HIPAA and puts you and the University at risk.

The HIPAA Security Rule prohibits a covered entity from assigning the same userID to multiple employees. The Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that maintains electronic protected health information, so that system access and activity can be identified and tracked by user. This pertains to workforce members within small or large healthcare provider offices, health plans, group health plans, and healthcare clearinghouses.

Remote Users

Do the HIPAA Security Rule requirements for access control, such as automatic logoff, apply to employees who telecommute or have home-based offices if the employee accesses electronic PHI?

Yes. Covered entities that allow employees to telecommute or work out of home-based offices and have access to electronic protected health information, must implement appropriate safeguards to protect the organization’s data. The automatic logoff implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the logoff implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate, or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure and document the rationale for this decision. The information access management and access control standards, however, require the covered entity to implement policies and procedures for authorizing access to PHI and technical policies and procedures to allow access only to those persons or software programs that have been appropriately granted access rights. Additional details about remote access to PHI can be found at: http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf

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
People have a plethora of computer accounts these days; e-mail accounts, online merchants, banks, professional organizations, social networking sites, etc. This leads to an overwhelming number of passwords and PINS that must be remembered. How can you securely keep track of them all? The answer is a Password Vault.

A Password Vault is a program that provides a central, secure location to store all these account passwords, PINS and other sensitive information and lock it all up with a single master password. With a Vault only the one master password need be remembered and all other passwords are securely encrypted in the Vault rather than being written down or stored insecurely on your computer.

There are many Password Vault programs available. ITaP’s Identity and Access Management Office recommends one such program called Password Safe (http://passwordsafe.sourceforge.net/) for Windows-based computers.

According to Cherry Delaney of ITaP Networks and Security:

- Password Safe features a simple, intuitive interface that lets users set up their password database in minutes.
- You can copy a password just by double-clicking, and pasting it directly into your application.
- Best of all, PasswordSafe is completely free: no license requirements, shareware fees, or other strings attached.

PasswordSafe was created by a noted cryptography and security expert. It has many convenient features, among them; ability to track password expiration and history, generate random passwords, and passwords that comply with a preset password policy. It also integrates nicely with a web browser.

The master password for the password manager must be complex and strong. It should be at least as strong as the most sensitive password stored inside. If the password manager stores any passwords that are subject to the requirements of a password policy, then the same requirements should be observed for the master password.

More info can be found at: http://www.purdue.edu/securepurdue/pswdManager.cfm

Communicating with a Patient’s Family, Friends, or Others Involved in the Patient’s Care

The Office for Civil Rights (OCR), which enforces compliance with the HIPAA Privacy Rule, has published guidance that explains when a health care provider is allowed to share a patient’s health information with the patient’s family members, friends, or others, identified by the patient, as involved in the patient’s care under the HIPAA Privacy Rule. Following, is the second of a series of questions and answers that were provided by OCR to illustrate appropriate handling of information under different circumstances. To read the guidance in its entirety, please access: http://www.hhs.gov/ocr/hipaa/provider_ffg.pdf

**Question:**

If the patient is not present or is incapacitated, may a health care provider still share the patient’s health information with family, friends, or others involved in the patient’s care or payment for care?

**Answer:**

Yes. If the patient is not present or is incapacitated, a health care provider may share the patient’s information with family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient. When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care. The health care provider may discuss only the information that the person involved needs to know about the patient’s care or payment.

**Examples:**

- A pharmacist may give a prescription to a patient’s friend who the patient has sent to pick up the prescription.
- A hospital may discuss a patient’s bill with her adult son who calls the hospital with questions about charges to his mother’s account.
- A health care provider may give information regarding a patient’s drug dosage to the patient’s health aide who calls the provider with questions about the particular prescription.

**BUT:**

- A nurse may not tell a patient’s friend about a past medical problem that is unrelated to the patient’s current condition.
- A health care provider is not required by HIPAA to share a patient’s information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.