PURDUE UNIVERSITY

HIPAA Advisory

http://www.purdue.edu/hipaa

March 2007 Newsletter

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.

Joan Vaughan
Purdue University Student Health Center

From the Director

Happy St. Patrick's Day to all of you. Spring is just around the corner and it will again be time for Privacy Assessments. I will begin scheduling these assessments to begin in May. They have been going very quickly and smoothly and I don't expect anything different, this year. I have also started a final phase of the security assessments, begun in 2006. This follow up includes creating an inventory of our current system logging practices, checking compliance with University password requirements and the creation of a list of potential risks for each area. Also, where security assessmen postponed due to OnePur involvement, will be completed in 2007.

HIPAA Basics - When Does HIPAA Apply?

With all of the talk about "HIPAA violations", many are confused about specifically what information HIPAA actually protects and when these protections apply.

COVERAGE

Medical facilities, (hospitals and doctor's offices) who bill electronically must comply with the HIPAA laws. When a medical facility is covered by HIPAA, the entire facility must comply.

Purdue, however, is a higher-education institution with the primary purpose of education. Purdue has the option of designating the entire University as covered by HIPAA or only those areas that meet certain coverage requirements.

Purdue has been designated as a "hybrid" entity. This means that HIPAA does not apply to all areas at Purdue, but only those areas that have been officially designated as "covered components". The HIPAA Privacy Compliance Office officially designates particular areas at Purdue as covered after assessing whether the area meets the coverage requirements. Only those designated areas, referred to as covered components, are obligated to comply with the HIPAA laws. The full list of covered components at Purdue can be found at: http://www.purdue.edu/hipaa/guidelines/coveredcomponents.shtml.

PROTECTED HEALTH INFORMATION

HIPAA only protects "individually identifiable health information" held or transmitted by a "covered component" or its business associate.

Also, all personally identifiable health information is not protected by HIPAA. HIPAA ***EXCLUDES*** protection of individually identifiable health information in:

- Education records covered by the Family Educational Rights and Privacy Act (FERPA), and
- Employment records held by a covered entity in its role as employer.

EXAMPLES

For example, if you as an employee in a covered component (i.e. PUSH), accessed and then shared treatment or healthcare information about an employee who was treated at PUSH, out of curiousity, this is a HIPAA violation because as part of a covered component, you accessed and then disclosed PHI without a proper business purpose or without a written authorization.

If HR receives information, for example, return to work documentation from an employee, the information would be covered by HR laws, not HIPAA (see exception above).

If an employee who is on medical leave, shares information about their own medical condition with employees who then share this information at work with others without permission, this may be a breach of confidentiality, but is not a HIPAA violation. In this case, the information was not protected health information cre ated within one of Purdue's covered components. The individual can share whatever private information about themselves that they wish to share.

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

Security Tips

ITaP's Security and Privacy area has provided information to help you better protect the security of your workstation. Following are some helpful tips found on the Secure Purdue website.

View email messages individually

Spam emails often contain code that automatically incites more spam or attempts to install viruses and spyware. Avoid this problem by viewing email messages individually, rather than in a previewing pane. To toggle the Preview Pane in Microsoft Outlook, click View»PreviewPane.

Ignore unsolicited emails

Spammers send emails that pretend to be from legitimate sources to trick you into providing your personal information. This practice is known as "phishing." Never click on links in an email. Phishers can make fake email links that:

> Browse to the legitimate web site, but sneak in a pop-up window from a phisher's web site that asks for personal info

> Browse to a fake web site that has a nearly identical look and address to the legitimate web site

> Cover up the browser address window with an image that makes it appear to be the legitimate web site

> Invisibly download a key-logging program that records and reports back every keystroke made on the computer, including entered passwords and credit card numbers

Avoid untrustworthy downloads

Virus writers use downloadable screensavers and other files to infiltrate computer systems. Free CDs may also harbor spyware and viruses.

Log off or turn off the computer

When you leave your computer, make sure to lock it (Windows key + L) or log off. If you are leaving for an extended period (a weekend, for example), turn the computer off.

Scrutinize attachments carefully

Email and instant messaging are major vehicles for viruses. Spammers are very skilled at making virus emails and attachments sound legitimate. Open only expected email attachments sent from known addresses, especially if the file extension of an attachment is .exe, .bat, .vbs, .pif, .scr, .cmd, .hlp, .lnk, or .com.

Visit the SecurePurdue Web site

Browse to http://www.purdue.edu/securepurdue for the latest in computer security and privacy

FAQ of the Month

Provided by the Office for Civil Rights
http://www.hhs.gov/ocr/hipaa/

Question:

May a health plan disclose protected health information to a person who calls the plan on the beneficiary's behalf?

Answer:

Yes. subject to the conditions set forth in 45 CFR 164.510(b) of the HIPAA Privacy Rule. The Privacy Rule at 45 CFR 164.510(b) permits a health plan (or other covered entity) to disclose to a family member, relative, or close personal friend of the individual, the protected health information (PHI) directly relevant to that person's involvement with the individual's care or payment for care. A covered entity also may make these disclosures to persons who are not family members, relatives, or close personal friends of the individual, provided the covered entity has reasonable assurance that the person has been identified by the individual as being involved in his or her care or payment.

A covered entity only may disclose the relevant PHI to these persons if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure; however, when the individual is not present or is incapacitated, the covered entity can make the disclosure if, in the exercise of professional judgment, it believes the disclosure is in the best interests of the individual.

For example:

- A health plan may disclose relevant PHI to a beneficiary's daughter who has called to assist her hospitalized, elderly mother in resolving a claims or other payment issue.
- A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm for the plan that the representative calling is assisting the beneficiary.
- A health plan may disclose relevant PHI to a Congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the Congressional office's assistance.
- A Medicare Part D plan may disclose relevant PHI to a staff person with the Centers for Medicare and Medicaid Services (CMS) who contacts the plan to assist an individual regarding the Part D benefit, if the information offered by the CMS staff person about the individual and the individual's concerns is sufficient to reasonably satisfy the plan that the individual has requested the CMS staff person's assistance.