PURDUE UNIVERSITY

HIPAA Advisory

http://www.purdue.edu/hipaa

March 2006 Newsletter

Joan Vaughan
Purdue University Student Health Center

From the Director

I would like to remind the liaisons that the HIPAA Privacy Compliance Office will soon be scheduling Privacy Assessments for each covered component to begin in May 2006.

Also, Security Assessments will be conducted in each HIPAA-covered area beginning in June of 2006 by ITaP Security and Privacy and the HIPAA Privacy Compliance Office. More details will be communicated prior to the meetings.

Relating to security, is an effort by ITaP to combine the HIPAA and GLBA security compliance efforts into one program. When complete, those departments who are affected by both HIPAA and GLBA will only face one security assessment annually instead of two.

Have a wonderful spring!

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.

New State Laws

Effective **July 1, 2006**, there are two new state laws that may directly impact your areas. The first limits the disclosure of social security numbers and the other requires notification when a breach of personal information occurs. These laws will be discussed at the next HIPAA Liaison Committee meeting on April 18, 2006.

RELEASE OF SOCIAL SECURITY NUMBER IC 4-1-11

The new law states that as a state agency, Purdue University may not disclose an individual's social security number (SSN) unless:

- the disclosure is expressly required by state law, federal law or court order,
- the individual expressly consents in writing to the disclosure,
- the disclosure is made to comply with the USA Patriot Act of 2001 or Presidential Executive Order 13224,
- the disclosure is to a commercial entity for the permissible uses set forth in the Drivers Privacy Protection Act, Fair Credit Reporting Act or Financial Modernization Act of 1999
- the disclosure is for the purpose of administration of the health benefits of a Purdue employee or the employee's dependents,
- A state law enforcement agency may, for purposes of furthering an investigation, disclose the SSN of an individual to any individual, state, local, or federal agency, or other legal entity.

The penalties for unlawful disclosure are severe!

An employee of a state agency who knowingly, intentionally, or recklessly discloses an SSN in violation of this law or makes a false representation to a state agency to obtain an SSN, commits a Class D felony.

An employee of a state agency who negligently discloses an SSN in violation of this law commits a Class A infraction.

Continued on Page 2

Purchasing New Software or Making Software or Process Changes?

If either the purchase of new computer software or changes to existing software are planned in your area, and that software stores or provides access to protected health information, please notify your HIPAA liaison immediately.

The HIPAA liaison should contact the ITaP Security and Privacy department to be sure that the software's security features are compliant with HIPAA, GLBA and FERPA regulations.

The liaison should also notify Joan Vaughan whenever there are material process changes planned in your area.

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 Reminder - Use of E-mail

There continue to be questions about when e-mail can be used and what information can be included when the topic includes protected health information. Following are some guidelines on this subject.

EMAIL GUIDELINES

All e-mail when sent at Purdue, even an e-mail that is sent to a staff member in the same building, is transmitted over the network, through an e-mail server and is stored on that server for long periods of time. This e-mail may be available as part of the public record, by subpoena or to a potential hacker, until purged from the server some months later. Also, some staff and students forward their e-mail to servers off campus using AOL or MSN addresses where length of storage and security practices vary.

HIPAA requires appropriate safeguards for confidential information that is transmitted electronically, typically encryption for e-mail. Purdue does not currently have an encryption solution that is widely avaible for use, therefore, you should use the following guidelines when considering e-mail for communications.

- Do NOT ever e-mail social security number, treatment information or other confidential information. This is NOT okay, even if the patient okays it.
- Do NOT ever e-mail test results to a patient.
- It is NOT appropriate to e-mail information regarding payment for specifically-named treatment procedures to a health plan member.

If you need to communicate with a patient and you wish to use e-mail, ask the individual in the e-mail to contact you by phone at a particular time. Your e-mail should be very general and should not include confidential or treatment-related information.

It is OKAY to e-mail appointment reminders, however, the reminder should be very general. A good example is: "This e-mail is to remind you of an appointment with your healthcare provider at PUSH on March 23, 2006 at 3:00pm. If you cannot keep your appointment, please call 494-1700 24 hours prior to the appointment." The person's name should not be used in case the mail is misdirected.

You can also direct an individual to pick up an item ordered with the following e-mail: The item that has been ordered for you by PUSH PT is available for you to pick up at.... Please call x12345 if you have any questions."

Additional guidance is available on the HIPAA website: http://www.purdue.edu/hipaa under Communication Guidelines. If you have specific questions about e-mail usage, call the HIPAA Privacy Compliance Office at x47113.

FAQ of the Month

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

Question:

Does the HIPAA Privacy Rule require that covered entities provide patients with access to oral information?

Answer:

No. The Privacy Rule requires covered entities to provide individuals with access to protected health information about themselves that is contained in their "designated record sets." The term "record" in the term "designated record set" does not include oral information; rather, it connotes information that has been recorded in some manner.

The Rule does not require covered entities to tape or digitally record oral communications, nor retain digitally or tape recorded information after transcription. But if such records are maintained and used to make decisions about the individual, they may meet the definition of "designated record set." For example, a health plan is not required to provide a member access to tapes of a telephone "advice line" interaction if the tape is maintained only for customer service review and not to make decisions about the member.

New State Laws...Continued

Continued from page 1

NOTICE OF SECURITY BREACH IC 4-1-11

Any state agency (i.e. Purdue) that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose *unencrypted personal information* was or is reasonably believed to have been acquired by an unauthorized person.

"breach of the security of the system" is defined as:
An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency.

"personal information" means:
an individual's:
(A) first name and last name, or
(B) first initial and last name, and
at least one of the following data elements:
A. Social Security number
B. Driver's license number or ID card number.
C. Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account.

The term does NOT include:

1. The last four digits of an individual's SSN
2. Publicly available information that is lawfully made available to the public from records of a federal or local agency.