Joan Vaughan
Purdue University Student Health Center

From the Director

I would like to provide for you a glimpse of the projects currently in process in the HIPAA Privacy Compliance Office.

Work is continuing to verify and document that appropriate safeguards and business associate agreements are in place for several software purchases by Purdue’s covered components: medical records systems for the IPFW Dental Clinics and 4 WL School of Nursing Clinics, a risk management system for Insurance Services Enterprises and shared use of White County Memorial Hospital’s medical records system by Monon and Delphi clinics to facilitate the partnership with their collaborating physicians.

Also, efforts are underway to conduct security assessments in areas where assessments were postponed due to implementation of the OnePurdue system: A/R, Purdue health plans at all campuses and the OnePurdue Initiative.

In addition, the online training utility, created by the Office of the Registrar is now under consideration for development in Blackboard. This will allow retirement of the WebServ server and provide a consistent platform for delivery of OnePurdue-related training.

I want to wish everyone a wonderful and safe holiday!

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

Disclosures to Interpreters

Information derived from guidance provided by the Office for Civil Rights http://www.hhs.gov/ocr/hipaa/

Providing clear communications to non-English-speaking individuals or those with physical limitations is challenging and the need to provide interpreters and understand the related HIPAA requirements becomes important. When a covered component uses an interpreter to communicate with an individual, there are several considerations in determining the appropriate paperwork needed.

Internal Staff of the Covered Component

Covered components may use and disclose protected health information for treatment, payment and health care operations without an individual’s authorization. A covered component might use a member of it’s own workforce (i.e., a bilingual employee or a contract interpreter on staff) to provide interpreter services to communicate with individuals who speak a language other than English or who are deaf or hard of hearing. In these cases, provision of these services will be considered part of health care operations and does not require written authorization.

External Business Associates or Business Support Components

When a covered component engages the services of a person or entity, who is not a member of Purdue’s workforce to perform interpreter services on its behalf, the covered component may disclose protected health information as necessary to the business associate if the covered component has obtained:

- a written HIPAA authorization from the individual, or
- a business associate agreement was executed between Purdue and the business associate prior to the disclosure. This agreement includes certain assurances that the business associate will safeguard the confidentiality of the health information that they receive while interpreting.

If the covered component uses staff from another department at Purdue, which is not covered by HIPAA to provide interpreter services, either

- a written HIPAA authorization from the individual must be obtained, or
- the department must be designated as a covered component (notify the HIPAA Privacy Compliance Office of this need).

Friends or Family Interpreters

In addition, a covered component may, without the individual’s written authorization, use or disclose protected health information to the patient’s family member, close friend, or any other person identified by the individual as his or her interpreter for a particular healthcare encounter. As with other disclosures to family members, friends or other persons identified by an individual as involved in his or her care, when the individual is present, the covered entity may obtain the individual’s agreement or reasonably infer, based on the exercise of professional judgment, that the individual does not object to the disclosure of protected health information to the interpreter.

(Continued, Page 2)
Disclosures to Interpreters...Continued

Other Considerations
Organizations that are subject to both HIPAA and Title VI must comply with the requirements of both laws, though not all HIPAA covered entities are recipients of federal financial assistance and thus, required to comply with Title VI; and not all recipients of federal financial assistance are also HIPAA covered entities, subject to the Privacy Rule. For information about the obligation of recipients of federal financial assistance to take reasonable steps to provide meaningful access to persons who are limited English proficient, see Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons available at http://www.hhs.gov/ocr/lep/. This guidance includes information for recipients of federal financial assistance about important considerations for determining the competency of interpreters, such as their understanding of applicable confidentiality requirements, that should be taken into account when using interpreters arranged by the provider or when individuals elect to use friends, family or others as interpreters.

HIPAA covered entities may also be required to comply with the Americans with Disabilities Act and/or Section 504 of the Rehabilitation Act of 1973, both of which have requirements for the provision of sign language and oral interpreters for people who are deaf or hard of hearing. The use of communications assistants as part of a Telecommunications Relay Service (TRS) was the subject of a previous FAQ available at http://www.hhs.gov/ocr/hipaa (click on Your Frequently Asked Questions About Privacy, and then search on “TRS”).

Security News - Policy Review and Input
IT Networks and Security facilitates the development of University information security policies and consults on information security compliance activities under federal, state, and local law.

Policies are reviewed by ITNS and by the policy subcommittee of the Security Officers’ Working Group. Draft policies are then presented to the University Security Officers’ Working Group. After appropriate review by these groups, a formal procedure is followed once a proposed policy is ready for formal review and presentation to the Purdue University President for signature.

Information security policies, standards, and guidelines are currently under review by the Security Officers group and are provided at the following link for members of the Purdue community to review and provide comment. It is recommended that staff who may wish to provide feedback, check the website monthly for new drafts to review.

http://www.purdue.edu/securepurdue/bestPractices/draftITPolicies.cfm

Comments regarding the draft policies should be sent to securepurdue@purdue.edu by the date indicated in the policy draft. ITNS and the policy subcommittee of the Security Officers’ Working Group will review and discuss all comments received by the due date indicated in the policy draft. The draft may undergo further revisions based on comments received.

FAQ of the Month

Question:
Will the HIPAA Privacy Rule hinder medical research by making doctors and others less willing and/or able to share with researchers information about individual patients?

Answer:
We do not believe that the Privacy Rule will hinder medical research. Indeed, patients and health plan members should be more willing to authorize disclosures of their information for research and to participate in research when they know their information is protected. For example, in genetic studies conducted at the National Institutes of Health, nearly 32 percent of eligible people offered a test for breast cancer risk declined to take it. The overwhelming majority of those who refused cited concerns about health insurance discrimination and loss of privacy as the reason. The Privacy Rule both permits important research and, at the same time, encourages patients to participate in research by providing much needed assurances about the privacy of their health information.

The Privacy Rule will require some covered health care providers and health plans to change their current practices related to documenting research uses and disclosures. It is possible that some covered health care providers and health plans may conclude that the Rule’s requirements for research uses and disclosures are too burdensome and will choose to limit researchers’ access to protected health information. We believe few providers will take this route, however, because the Common Rule includes similar, and more rigorous requirements, that have not impaired the willingness of researchers to undertake Federally-funded research. For example, unlike the Privacy Rule, the Common Rule requires an Institutional Review Board (IRB) review for all research proposals under its purview, even if informed consent is to be sought. The Privacy Rule requires documentation of IRB or Privacy Board approval only if patient authorization for the use or disclosure of protected health information for research purposes is to be altered or waived. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.