From the Director

The Office of HIPAA Privacy Compliance is currently working with area liaisons to complete the preparations for coverage of the following areas:

* the School of Nursing (HIPAA Liaison Rhoberta Haley), and
* the Speech, Language and Hearing Sciences Department, (HIPAA Liaisons Barbara Solomon and Lata Krishnan).

Coverage will be effective January 1, 2006.

Also, the office is continuing to assist the Employee Wellness department with preparations for the new Health Risk Assessment Initiative. This service is expected to assist health plan members in making significant improvements in their health and result in substantial cost savings for the health plan.

I hope that you and your families enjoy the holidays and have a safe and prosperous New Year!

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.

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 Policy 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](http://www.purdue.edu/hipaa) or contact: Joan Vaughan, Director, HIPAA Privacy Compliance telephone: (765) 496-1927 e-mail: jvaughan@purdue.edu

Health Information Technology


President’s Vision for Health IT

In April 2004, President George W. Bush revealed his vision for the future of healthcare in the United States. The President’s plan involves a health care system that puts the needs of the patient first, is more efficient, and is cost-effective. The President’s plan is based on the following tenets:

- Medical information will follow consumers so that they are at the center of their own care
- Consumers will be able to choose physicians and hospitals based on clinical performance results made available to them
- Clinicians will have a patient’s complete medical history, computerized ordering systems, and electronic reminders
- Quality initiatives will measure performance and drive quality-based competition in the industry
- Public health and bioterrorism surveillance will be seamlessly integrated into care
- Clinical research will be accelerated and post-marketing surveillance will be expanded.

The president’s Vision for Health IT clarifies the need for HIPAA Privacy and Security Rules. Health information, stored electronically and available almost any time from anywhere, requires significant and consistent security safeguards. Privacy rules are necessary to specify where information can be shared, with whom, for what purpose and when authorizations to disclose are required by the patient. As the vision develops, you can expect adjustment of the existing rules and development of new rules to support the vision.
Employee Confidentiality

As you know, the confidentiality of patient/employee health information is all of our responsibilities. When you see or hear information about a patient or employee’s health while performing your jobs, you CANNOT disclose this information to your friends or family or to anyone else who does not have a legitimate need to know.

Consider some of the following reminders regarding the handling of confidential information.

- Conduct confidential verbal conversations in a private area or room.
- NEVER use or disclose confidential information for any personal purpose or out of curiosity, or allow others to do so. If you see another staff member in violation, please report to the HIPAA Privacy Compliance Office, x47113 so that the incident can be investigated.
- Keep your user id and password confidential. Never disclose to anyone or allow anyone else access to view or alter information under your identity. Passwords should NEVER be posted near the work area or in a place that is easily accessible by other people.
- Documents containing PHI should not be left in open areas or on desks where they can easily be seen by passers by. Place these documents in folders, turn them over or place a sheet of paper on top. Documents should be filed in a secure location when not in use.
- Always verify the identity of an individual when conveying information to them over the phone or in person. Follow the approved procedures for your area. If you don’t know what they are, ask your supervisor.

Our customers are relying on us to safeguard their information. Please make this a priority in the work that you do.

Confidentiality of protected health information is serious business! Violations of Purdue’s HIPAA Confidentiality Agreement will subject the employee to possible sanctions up to and including termination. HIPAA violations may result in Purdue being fined by Health and Human Services and criminal charges may be pursued by the Department of Justice.

FAQ of the Month

Question:

Does the HIPAA Privacy Rule permit a covered entity or its collection agency to communicate with parties other than the patient (e.g., spouses or guardians) regarding payment of a bill?

Answer:

Yes. The Privacy Rule permits a covered entity, or a business associate acting on behalf of a covered entity (e.g., a collection agency), to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. Therefore, a covered entity, or its business associate, may contact persons other than the individual as necessary to obtain payment for health care services. See 45 CFR 164.506(c) and the definition of “payment” at 45 CFR 164.501. However, the Privacy Rule requires a covered entity, or its business associate, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of protected health information. See 45 CFR 164.502(b), 164.514(d), and 164.522.

Recruiting Subjects for Research

A question frequently asked by researchers is whether they can recruit prospective research participants using a covered entity’s PHI.

The preparatory research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. As such, a researcher who is an employee or a member of the covered entity’s workforce could use protected health information to contact prospective research subjects. However, this does not permit the researcher to remove protected health information from the covered entity’s site. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information. Therefore, covered health care providers and patients may discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization.

However, a researcher who is not a part of the covered entity may NOT use the preparatory research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB. The IRB or Privacy Board waiver of authorization permits the partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects. Also, a member of the covered entity’s workforce may recruit potential subjects on behalf of the researcher.

Purdue University is an equal access/equal opportunity university