June 2005 Newsletter

From the Director

HIPAA compliance activities during the last quarter have focused on University compliance with the HIPAA Security Rule and the 2005 annual privacy reassessment. Follow up work is continuing on the security assessment and the reassessment of Purdue’s compliance with the Privacy Rule is nearly complete.

Thanks to all of the areas for their cooperation and efforts during this time. Hopefully, our work has not caused too much disruption in your areas.

The next new project is to plan for implementation of the required National Provider Identifier. Compliance is due by May 23, 2007 and will impact only our health care providers. More information will be provided in the future.

Have a great summer!

Joan Vaughan
Purdue University Student Health

Requirements for Marketing


The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing. So as not to interfere with core health care functions, the Rule distinguishes marketing communications from those communications about goods and services that are essential for quality health care.

The Privacy Rule addresses the use and disclosure of protected health information for marketing purposes by:

- Defining what is “marketing” under the Rule;
- Excepting from that definition certain treatment or health care operations activities;
- Requiring individual authorization for all uses or disclosures of protected health information for marketing purposes with limited exceptions.

What is “Marketing”?  

The Privacy Rule defines “marketing” as making “a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.” Generally, if the communication is “marketing,” then the communication can occur only if the covered entity first obtains an individual’s “authorization.” This definition of marketing has certain exceptions.

What Else is “Marketing”? Marketing also means: “An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service.”

(continued Page 2)

Purchasing New Software or Making Software Changes?

If you are planning to either purchase new computer software or make changes to existing software in your area and that software stores or processes 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 will also notify Joan Vaughan for consideration of process changes.

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
service that encourages recipients of the communication to purchase or use that product or service.” This part of the definition to marketing has no exceptions. The individual must authorize these marketing communications before they can occur. Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.

What is NOT “Marketing”?

The Privacy Rule carves out exceptions to the definition of marketing under the following three categories:

1. A communication is not “marketing” if it is made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about:
   - The entities participating in a health care provider network or health plan network;
   - Replacement of, or enhancements to, a health plan; and
   - Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

This exception to the marketing definition permits communications by a covered entity about its own products or services.

2. A communication is not “marketing” if it is made for treatment of the individual.

3. A communication is not “marketing” if it is made for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

For any of the three exceptions to the definition of marketing, the activity must otherwise be permissible under the Privacy Rule, and a covered entity may use a business associate to make the communication. As with any disclosure to a business associate, the covered entity must obtain the business associate’s agreement to use the protected health information only for the communication activities of the covered entity.

These are general rules regarding marketing and its HIPAA implications. The HIPAA Compliance Office can be contacted at x47113 to discuss specific issues related to your area.

FAQ of the Month

Provided by the Office of Civil Rights

http://www.hhs.gov/ocr/hipaa/

Question:

May physicians offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

Answer:

Yes. Covered entities, such as physician’s offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician).

When is a Researcher Covered by HIPAA?

Derived from the Office of Civil Rights

http://www.hhs.gov/ocr/hipaa/

A researcher is a covered health care provider under HIPAA if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule.

For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf.

Researchers are also covered by HIPAA as a member of the workforce of an area designated as covered by Purdue University.

In addition, there are specific requirements that must be met, prior to a researcher obtaining protected health information from an entity that is covered by HIPAA.

For assistance in determining how HIPAA impacts your particular situation, call the HIPAA Privacy Compliance Office at x47113.