Joan Vaughan
Purdue University Student Health Center

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.

**Requests for Confidential Communications**

It is the policy of Purdue University’s covered health care providers to accept and accommodate reasonable requests by individuals to receive protected health information through alternative means or at alternative locations.

**Health Care Providers** may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

**Purdue’s health plan(s)** will accept verbal requests for confidential communications on a single-event basis. The health plans will require that all requests for confidential communications include a statement that disclosure of all or part of the information, to which the request pertains, could endanger the individual.

**Examples** of these kinds of requests are:

- a request to send bills for treatment to an on-campus address
- a request to return a phone call to a specific phone number

Your HIPAA Privacy Liaison should be notified immediately, if a request is received to permanently change the method of communication with an individual. These requests are required in writing and will be reviewed by the Director of HIPAA Privacy Compliance.

All HIPAA forms and procedures can be found on the HIPAA website:

http://www.purdue.edu/hipaa

**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
Indians have the right to request a restriction of the use and disclosure of their protected health information and for the request to be promptly reviewed.

Purdue University is not required to agree to the restriction, but if approved, all covered components must abide by the restriction.

All requests for restricted use of PHI will be reviewed by the Director, HIPAA Privacy Compliance.

If a request is received, notify your HIPAA Liaison immediately. Your liaison can help you follow the HIPAA restriction procedure.

Question:
Is an entity that is acting as a third party administrator to a group health plan a covered entity?

Answer:
No, providing services to or acting on behalf of a health plan does not transform a third party administrator (TPA) into a covered entity. Generally, a TPA of a group health plan would be acting as a business associate of the group health plan. Of course, the TPA may meet the definition of a covered entity based on its other activities (such as by providing group health insurance). See 45 CFR 160.103.

No, the Privacy Rule does not require these types of structural changes be made to facilities.

Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard.

For example, the Privacy Rule does not require the following types of structural or systems changes:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
- Encryption of telephone systems.

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.

- In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonably use cubicles or shield-type dividers, rather than separate rooms, or providers could add curtains or screens to areas where discussions often occur between doctors and patients or among professionals treating the patient.