Purdue's Environmental Health
Protected Health Information Data Handling and Disposal Guidelines

All employees who have been designated as covered by HIPAA are responsible for maintaining the confidentiality and security of patient health information. Special protections exist for protected health information and these guidelines specify appropriate data handling and disposal procedures to be used by Environmental Health staff to safeguard this information.

These guidelines apply to the individually identifiable health records that are accessed or maintained by the Environmental Health department and are protected by HIPAA and is consistent with existing University handling requirements. This information is defined in the Environmental Health Designated Record Set policy. Refer to this policy when considering to which records the following procedures apply.

DATA ACCESS

- Only Environmental Health staff designated as covered by HIPAA are allowed to access the information defined in the designated record set without prior patient written authorization or unless the purpose falls within the scope of allowable disclosures under HIPAA.

- All patient information is considered confidential and only the information needed for the intended purpose should be used by, and disclosed to, covered staff members who have a “need to know” (i.e. Minimum Necessary). A staff member with a “need to know” is defined as someone who needs the information because the information is directly related to the duties and activities the person is required to perform as described in their job description. Without such information the staff member would not be able to carry out these functions.

- Environmental Health staff who are patients of the clinics or who have dependents, family members, co-workers, or friends who are patients of the clinics must follow standard procedures, applicable to all patients, for accessing their own patient billing information or the patient billing information of their dependents, family members, co-workers, or friends.

- Staff members may not discuss patient information with their friends, family members, spouses, religious leaders, or any other individual unless allowable by HIPAA (i.e. have knowledge that an individual is participating in decisions related to treatment or payment for healthcare for the patient or a power of attorney indicating that the individual is the patient’s representative.)

- Inappropriate use or disclosure of individually identifiable health information will be reported to the PUSH HIPAA liaison or to the Director, HIPAA Privacy Compliance using the inadvertent disclosure tracking process. The University may apply sanctions to employees who violate HIPAA policies and procedures.

- Protected health information should never be sent via unencrypted e-mail. Please refer to the HIPAA Communications Guidelines for more detail: http://www.purdue.edu/push/HIPAA/Guidelines/files/communicationguidelinesforhipaa.pdf

- ITaP has provided a secure tool, File Locker, to be used for electronic communications containing protected health information: http://www.purdue.edu/push/HIPAA/FormsProcedures/Data/index.html
If you need to communicate with a patient or health plan member 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 information.

Periodically, individuals will e-mail confidential information to you. If a patient sends an e-mail requesting confidential information, you can modify and use the following sample text to respond:

Federal and state regulations require encrypted e-mail systems for certain confidential communications. Since Purdue e-mail communications are not encrypted, it is the policy of Purdue University not to use e-mail to discuss confidential health or benefits information. We are sorry if this causes inconvenience for you.

Please call the xxxxxxx office at (765) 49x-xxxx to speak with us or dial (765) xxx-xxxx to contact the xxxx switchboard.

**Procedures for Accessing the Protected Health Information**

- The records will only be accessed by covered staff and only for legitimate business purposes.
- The records are maintained in locked cabinets in the office and full-time Environmental Health staff have keys to the cabinet.

**Research Disclosures**

- In the unlikely event that a request for PHI would be received for the purposes of research, the researcher will be referred to the covered component that owns the information for proper response to the request.

**DOCUMENT STORAGE**

Documents containing PHI are maintained in the Environmental Health office in a cabinet that is locked when staff are out of the office.

**MAILING OF DOCUMENTS**

When documents are mailed via campus mail or via external mail carrier, no classification marking should be used to indicate the contents of the envelope and the envelope should be sealed in such a way that tampering would be indicated upon receipt.

**DISPOSAL**

- All protected health information will be maintained for a minimum of 6 years. At least annually, the department director will oversee review of the records to determine eligibility for disposal.
- Employees will never copy files containing PHI to an unencrypted laptop or mobile device (i.e. palm Blackberry or FLASH drives). If data is stored on CDs or other removable media, this media will be erased or destroyed beyond the ability to recover, as specified in the University Data Classification and Handling Guidelines before reuse or disposal.