Purdue's Public Records Office
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 (PHI) and these guidelines specify appropriate data handling and disposal procedures to be used by Public Records staff to safeguard this information.

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

RECORD ACCESS

- Only Public Records 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 (i.e. healthcare operations).

- All individually identifiable health information obtained from a HIPAA-covered provider or covered health plan 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.

- Public Records employees who are patients of a covered clinic or who have dependents, family members, co-workers, or friends who are patients of the clinic must follow standard procedures, applicable to all patients, for obtaining access to their own patient information or the patient information of their dependents, family members, co-workers, or friends from the clinic that provided service. The same requirement applies to health plan member information maintained by Purdue’s covered health plans.

- Public Records employees may not discuss PHI with their friends, family members, spouses, religious leaders, or any other individual that would violate the HIPAA Privacy Rule.

- Inappropriate use or disclosure of PHI will be reported to the Public Records HIPAA liaison or to the HIPAA Privacy Officer using the inadvertent disclosure tracking process. The University may apply sanctions to employees who violate HIPAA policies and procedures.

- 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.

- If a patient sends an e-mail or text requesting confidential information, you can modify and use the following sample message to respond:
Regulations require encrypted messaging systems for confidential communications. Since Purdue e-mail/text communications are not encrypted, it is the policy of the Purdue [department name] not to use e-mail/text for sharing confidential information. We are sorry if this causes inconvenience for you in receiving information from us.

Please call the xxxxxxx office. [Dept name] office hours can be found at:

http://www.purdue.edu/xxxx

RESEARCH DISCLOSURES

- Should there be a request for PHI to the Public Records Office to be used for research, the researcher will be referred to the clinic or health plan office that owns the information for proper response to the request.

PROCEDURES FOR ACCESSING THE MEDICAL RECORD

- PHI requested within a public records request will be provided pursuant to a valid HIPAA authorization or subpoena. The HIPAA Privacy Officer will review HIPAA authorizations that are not on Purdue’s official authorization form, prior to disclosures. If the authorization is deemed valid, the information will be requested from the clinic or health plan that owns the data.

- All subpoenas requesting PHI will be reviewed by University counsel prior to collection or disclosure of the data. If the subpoena is deemed valid, the information will be requested from the clinic or health plan that owns the data.

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

- HIPAA authorizations or subpoenas relating to PHI and a copy of the information disclosed will be filed and maintained for six years from the date of receipt of the request by Purdue or effective date, whichever is later.

- At least annually, the public records director will oversee review of the records to determine eligibility for disposal. The paper records to be purged, will be placed in locked containers intended for confidential destruction according to approved Purdue Recycling procedures. Video tapes, cds or other electronic media will be provided to Business Services Computing, who will physically destroy beyond the ability to recover the data. DVDs and other media are destroyed physically by shredding.

- 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.