Purdue's Pharmacy

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 Pharmacy staff to safeguard this information.

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

RECORD ACCESS

- Only Pharmacy 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. treatment).

- All Pharmacy 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 Pharmacy 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.

- Pharmacy employees who are patients of the Pharmacy or who have dependents, family members, co-workers, or friends who are patients of the Pharmacy must follow standard procedures, applicable to all patients, for accessing their own patient information or the patient information of their dependents, family members, co-workers, or friends. Patient records should be requested through the Pharmacist on duty. If the request is made by someone other than the patient, either a HIPAA authorization or a power of attorney indicating that the employee is the patient’s representative would need to be present in the file.

- 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 healthcare decisions or payment for healthcare for the patient or a power of attorney indicating that the employee is the patient’s representative.)

- Patient information is protected by law. Inappropriate use or disclosure of Pharmacy individually identifiable health information will be reported to the Pharmacy HIPAA liaisons or to the Director, HIPAA Privacy Compliance using the inadvertent disclosure tracking process. The University may apply sanctions to employees who do not follow 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.
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.

Research Disclosures

Covered staff who are conducting research that has been approved by Purdue’s IRB, authorized by the patient or pursuant to a waiver of authorization requirements, may access the patient records directly to obtain the data that they need to conduct the research. The researcher will be responsible for using only the data that is listed in the HIPAA authorization and approved for use by the IRB.

In the case of research disclosures that require tracking (i.e. where a waiver of authorization has been granted), the researcher will be responsible for providing the tracking documents to the Pharmacy HIPAA liaison, who will ensure that the tracking documents are filed.

Non-covered staff will be required to request data from the Pharmacy HIPAA liaison for use in Purdue IRB approved research. When a waiver of authorization requirements is granted and tracking of disclosures required, the tracking documents will be provided by the researcher to the HIPAA liaison. The HIPAA liaison will ensure that the tracking documents are filed.

In the case where use of a limited data set is required, the Purdue IRB approvals will be presented by the researcher to the HIPAA liaison. A data use agreement will be provided to the researcher for signature, by the HIPAA liaison. The data use agreement will be maintained by the HIPAA liaison for 6 years from date of creation and a copy provided to Purdue’s IRB by the researcher.

Preparatory to Research

Use or disclosure of protected health information may be sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research.
**Covered** staff who are considering research may access the patient records directly to obtain the data that they need for preparatory to research purposes. The data may not be used for research until after the researcher has obtained the appropriate approvals from Purdue’s IRB.

**Non-covered** staff will be required to request information from the Pharmacy director for preparatory to research purposes. No identifiable data may be provided to the researcher without appropriate approvals from Purdue’s IRB.

**Procedures for Accessing the Patient Record**

- The patient record is stored in the Pharmacy QS/1 system and will be maintained for a minimum of 7 years. The QS/1 server is located in a back room in the Pharmacy. The server is cabled to the floor and the room and Pharmacy locked after hours and when staff are away from the area.
- Patient records will only be accessed by covered staff and students and only for legitimate business purposes.
- Information in the designated record set (refer to the Pharmacy Designated Record Set documentation for the definition) will not be removed from the Pharmacy building, except under these circumstances:
  - A copy being provided to the patient or their representative, as requested.
  - Records released pursuant to a valid HIPAA authorization, subpoena, discovery request or other lawful process.
  - Records will be disclosed to insurance companies or others for the purpose of obtaining payment.
  - Records may be forwarded to other providers or pharmacies as requested and authorized by the patient.
  - Reporting to the state or federal government as required for Public Health purposes.

**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 information listed in the patient record will be maintained electronically for a minimum of 7 years. Any paper containing PHI to be purged, will be placed in locked containers intended for confidential destruction according to approved Purdue Recycling procedures. Electronic media will be provided to Pharmacy Technical Services, who will physically destroy beyond the ability to recover the data.
- 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.