Purdue's Student Health Center
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 PUSH staff to safeguard this information.

These guidelines apply to the individually identifiable health records that are maintained by the Purdue Student Health Center and are protected by HIPAA and is consistent with existing University handling requirements. This information is defined in the PUSH Designated Record Set policy. Refer to this policy when considering to which records the following procedures apply. For convenience, the term patient(s), below, will refer to both medical patients and mental health clients of the Purdue University Student Health Center. The reference to health information includes both physical and mental health.

RECORD ACCESS

- Only PUSH 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 clinic 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 clinic 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.

- Clinic employees who are patients of the 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 accessing their own patient information or the patient information of their dependents, family members, co-workers, or friends. A copy of the health record should be requested through the clinician who is providing treatment. If the request is made by someone other than the patient, either a HIPAA authorization would need to be present in the file, form indicating participation in health healthcare decisions or payment for health care or a power of attorney indicating that the employee is the patient’s representative.

- 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 and the standards of medical or mental health ethics. PUSH employees may be subject to disciplinary action up to and including termination if they violate HIPAA policies and procedures.

- Inappropriate use or disclosure of clinic individually identifiable health information will be reported to the PUSH HIPAA liaisons or to the HIPAA Privacy Officer 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 passersby. 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, FileLocker, 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 health 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 appropriate speech or audiology HIPAA liaison, who will ensure that the tracking documents are filed in each patient record.

Non-covered staff will be required to request data from the appropriate speech or audiology 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 responsible for that particular area of the clinic. The HIPAA liaison will ensure that the tracking documents are filed in the appropriate patient health records.

In the case where use of a limited data set is required, the Purdue IRB approvals will be presented by the researcher to the appropriate 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 health 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 clinic supervisors 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 Health Record**

- The health record will be stored either in an electronic health record system or in cabinets located in the clinics behind the reception area and will be maintained for a minimum of 7 years. The cabinets will be locked after hours and when staff are away from the area.

- Recordings of treatment sessions *used for purposes of treatment or diagnosis* will be considered part of the health record and stored with other health record documentation or as in the case with mental health session recordings, in a designated electronic storage location.

- The records will only be accessed by covered staff and only for legitimate business purposes.

- Records may not be accessed for research purposes unless the appropriate approvals have been obtained from Purdue’s IRB and patient authorizations, waiver of authorization requirements or data use agreement obtained and as specified below. Research requests must be forwarded to the HIPAA liaison to verify that all approvals and appropriate documentation is on place prior to disclosure.

- Information in the designated record set (refer to the PUSH Designated Record Set documentation for the definition) will not be removed from the building, except under these circumstances:
  - A copy being transferred pursuant to an authorization.
  - Records faxed to another location for continuing care, to obtain payment, for legal purposes or as otherwise allowed under HIPAA or State law.

- When physically taken off-site, folders or other materials should be placed in an enclosed container and labeled confidential to prevent from inadvertent loss of materials. The materials must be returned promptly to the clinic health record when no longer needed off-site.

- If faxed, the PUSH fax procedures will be followed.
Procedures for Storing Student Training Recordings

- Recordings of treatment sessions used solely for purposes of critiquing clinician procedures and not for treatment or diagnosis purposes will not be considered part of the health record. These recordings, however, contain individually identifiable health information and are considered part of the designated record set and should not be accessed by non-covered staff.

- A HIPAA authorization should be signed by patients, authorizing the disclosure of the recording for training purposes. Care must be taken to use and disclose the contents of the recording only as specified in the HIPAA authorization.

- Students or their supervisors will be required to enter information on a check out card located in the clinic front office patient file cabinet, when removing a recording from the cabinet, indicating the name of the person removing the information, the date of removal and the first 2 initials of the first and last name of the client. The recording should be labeled on the outside with the first 2 initials of the first and last name of the client. Recordings should be returned to the recording cabinet within 24 hours. The recordings should only be viewed in the PUSH or PSYC buildings in private areas, away from where others could view the session, or in an appropriate classroom setting, as specified in the HIPAA authorization.

- The recording must not be copied on to a computer outside of the PUSH or CAPS clinics or onto other media.

- Recordings of treatment sessions used for purposes of treatment or diagnosis will be considered part of the health record.

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 health record will be maintained for a minimum of 7 years. At least bi-annually, the clinic 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 PUSH technical services, who will physically destroy beyond the ability to recover the data. DVDs and other media are destroyed physically by shredding them.

- 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.