PURDUE UNIVERSITY

HIPAA

HIPAA Compliance
At Purdue

Purdue's Calumet Technological Infrastructure Services
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 Calumet Technological Infrastructure Services (IS) staff to safeguard this information. Additional information is provided in the HIPAA Communications and Office Security Guidelines, http://www.purdue.edu/push/HIPAA/Guidelines/files/communicationguidelinesforhipaa.pdf. All staff must comply with the guidelines in that document, as applicable to the work that you do.

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

RECORD ACCESS

- IS staff designated as covered by HIPAA, are authorized to provide workstation support to the HIPAA covered departments at Purdue Calumet. Staff will not access protected health information directly, but may have incidental access as a consequence of troubleshooting, providing maintenance or hardware replacement for departmental workstations.
- Generally, IS staff have no need to look at the protected health information maintained by the department in computers or in paper files. All protected health information is considered confidential and IS staff who come across protected health information as they perform their business function, will not share this information with anyone except the data owner. IS staff may not discuss protected health information with their friends, family members, spouses, religious leaders, or any other individual unless allowable by HIPAA (e.g. to the data owner in order to determine where to properly store the data).
- Protected health information is protected by law. Inappropriate use or disclosure of individually identifiable health information will be reported to the Calumet HIPAA liaison or to the HIPAA Privacy Officer using the inadvertent disclosure tracking process. IS employees may be subject to disciplinary action up to and including termination if they violate HIPAA policies and procedures.
- Periodically, individuals will e-mail confidential information to you. If a patient sends an unencrypted e-mail requesting confidential information, you can modify and use the following sample text to respond:

  > Federal 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 (xxx) 49x-xxxx to speak with us or dial (xxx) xxx-xxxx to contact the xxxx switchboard.

RESEARCH DISCLOSURES

- Should there be a request for PHI to the Calumet Technical Infrastructure Services office to be used for research, the researcher will be referred to the covered component that owns the information for proper response to the request.

ELECTRONIC TRANSFERS OF DATA

- Should there be a situation when data containing PHI, needs to be electronically transmitted outside of the subnet where the workstation or server is located that stores the data, the data must be encrypted prior to the transfer. FileLocker is an appropriate tool to use in these instances.

DISPOSAL

No documents containing PHI are used or maintained by Calumet Technological Infrastructure Services, therefore no disposal method for documents is required.

For electronically stored data, IS has a written disposal procedure that is used when all hardware needs to be cleaned. If computer equipment leaves the University, the hard drive will be destroyed prior to disposal. If the equipment is transferred to another user, the hard drive is wiped using a system that meets the DOD standard. CDs are shredded if requested by the user.

Employees will never copy files containing PHI to a laptop or mobile device (i.e. palm Blackberry or FLASH drives), unless other means of storage are unavailable and prior approval has been obtained from the supervisor. PHI should never be stored on a local workstation drive. If data is stored on CDs, 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.