

**PURDUE UNIVERSITY
HIPAA POLICIES AND PROCEDURES
FOR BUSINESS SUPPORT COMPONENTS**

_____, a business support component ("Business Support Component") designated by the University Policy regarding Compliance with HIPAA Privacy Regulations, adopts and implements these policies and procedures to ensure that protected health information in any form, including records, oral communications and electronic and other media are secure and protected.

1. Policy Regarding Confidentiality and Security of Protected Health Information

As a designated "covered component," it is the obligation of Business Support Component to comply with the requirements of the Purdue University's Policy regarding Compliance with HIPAA Privacy Regulations. This policy applies to all staff members who have access to protected health information as a result of services provided to one or more of the Healthcare Providers (i.e., PUSH, Purdue Pharmacy, Purdue's School of Nursing Nursing Centers, Purdue's SLHS Audiology and Speech-Language Clinics, Lafayette Street Family Planning Clinic, Lafayette Street Dental Clinic or IPFW Dental Hygiene Clinic) or any of the Health Plan Covered Components (i.e., medical plans, vision plan, pharmacy plan, health care flexible spending account plan, employee assistance programs, employee wellness programs, and worklife). These designated covered components may change from time to time, so all staff members are required to be familiar with those portions of the University that are designated as "covered components" and to apply these procedures to any protected health information obtained from a covered component. The full list of covered components can be viewed at <http://www.purdue.edu/hipaa>

The term "protected health information" is broadly defined in the University Policy regarding Compliance with HIPAA Privacy Regulations, and includes identifying information such as names and addresses. The University Policy defines protected health information as:

Individually identifiable health information, in any received or created as a consequence of providing healthcare services or health plan benefits (including demographic information). *Protected health information may include information used for research purposes, if that information identifies or could be used to identify a human research subject.*

It is the policy of this Business Support Component to protect the privacy and security of any protected health information that it accesses, uses, or discloses. All employees are required to keep protected health information private and confidential, and employees shall limit use and disclosure of protected health information to those purposes necessary to perform their job functions, and to follow the policies and procedures outlined below. Employees with access to protected health information will receive training on the HIPAA Privacy Regulations and these

policies and procedures. Employees with access to protected health information shall be required to sign an approved confidentiality agreement, and appropriate sanctions will be imposed upon any employee who violates the confidentiality agreement or this policy.

2. Notice of Privacy Practices

These policies and procedures are designed to be in compliance with the Notices of Privacy Practices for the Healthcare Providers and the Health Plans. Copies of the Notices of Privacy Practices are posted on the Purdue website at www.purdue.edu. Both Notices are binding on Business Support Component, and all employees are expected to read and follow all applicable practices described in the Notices or Privacy Practices.

3. Minimum Necessary Requirement

Except as otherwise permitted in this document, uses and disclosures of protected health information must be limited to the "minimum necessary to accomplish the intended purpose." The minimum necessary standard is not applicable to uses, disclosures or requests by a healthcare provider for "treatment" purposes. Only those employees who need access to protected health information to carry out their duties shall be permitted access to protected health information, and all protected health information shall be maintained in a secure environment to ensure limited access to protected health information and to avoid incidental disclosures of protected health information. The minimum necessary requirement does not apply to information disclosed pursuant to a written authorization from the individual, or to Health and Human Services for compliance audits.

4. Administration Requirements

A. Privacy Officer

The University has appointed a Privacy Officer, and the Business Support Components have designated a Privacy Liaison in each area to interact with the Privacy Officer on HIPAA privacy issues or rights. The Privacy Officer is responsible for the development, implementation and oversight of the HIPAA policies and procedures of Business Support Components. All staff members are expected to work cooperatively with the Privacy Officer and the Privacy Liaison, and to respond promptly and thoroughly to any requests of the Privacy Officer concerning HIPAA Privacy issues, training or investigation of complaints. Any questions or concerns about HIPAA Privacy issues or these policies and procedures should be directed to the Privacy Liaison. The Privacy Liaison for Business Support Components will maintain all documentation required by the HIPAA Privacy Regulations or requested by the Privacy Officer for a period of 6 years.

B. Prohibition against Retaliation

Retaliation against individuals who exercise their rights under the HIPAA Privacy Regulations is absolutely prohibited, and employees shall not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any such individual or any

person who files a complaint, testifies or participates in investigation or compliance review, or opposes any act or practice made unlawful by the HIPAA Privacy Regulations.

C. Complaints

Individuals have a right to complain about the University's privacy practices. Any staff member who receives a complaint about Business Support Group's compliance with the HIPAA Privacy Regulations or Business Support Group's privacy practices shall direct the individual to the Privacy Liaison who will immediately forward the complaint to the Privacy Officer for investigation and response. All staff members are expected to cooperate fully in the investigation of any such complaints.

D. Training of Employees

The Privacy Officer in cooperation with the Privacy Liaison shall provide training to all staff members about the HIPAA Privacy Regulations and these policies. All staff members who have access to protected health information will be required to participate in all training provided, and to promptly provide all documentation requested about participation in the training. New employees who have access to protected health information will be trained as soon as reasonably possible after being hired.

E. Mitigation

Any improper or unauthorized use or disclosure of protected health information must be reported immediately to the Privacy Officer. If a staff member is notified that protected health information has been misused by an employee or a business associate, the staff member must notify the Privacy Liaison who will report the misuse or wrongful disclosure to the Privacy Officer. Staff members shall cooperate fully in any investigation of misuse or wrongful disclosure, and shall take all reasonable steps to rectify and minimize the impact of the misuse or unauthorized disclosure.

F. Physical Safeguards

Staff members are required to protect the security of protected health information from unauthorized access to, use or disclosure. Employees are not permitted to do any of the following:

1. Remove any records, reports or copies of documents containing confidential or personal information from their storage location except as needed for the performance of job duties;
2. Release user identification codes or passwords to unauthorized users, or allow anyone to access or alter information under the employee's identity;
3. Use personal or confidential information to engage in illegal activities or to harass anyone;

4. Allow unauthorized use of information maintained, stored or processed in any electronic file, medical file, student file or computer system;
5. Access, use or disclose confidential information for any personal purpose or out of curiosity, or allow others to do so by giving them the employee's access codes, passwords or use of employee's equipment for any purposes not essential to the employee's work.

5. Authorizations and Restricted Uses or Disclosures

A. Authorizations

Any uses or disclosures of protected health information outside the scope of normal operations should be referred to the Privacy Liaison designated by Business Support Component to determine whether the individual who is the subject of the protected health information must first sign a written authorization. The written authorization must be in a form approved by the Privacy Officer.

B. De-Identified Information

De-identified information is not "protected health information" as defined in the HIPAA Privacy Regulation, and is therefore not subject to the HIPAA Privacy Regulations. However, information is not considered de-identified unless all of the following identifying information is removed:

- Name
- Geographic subdivision smaller than a state including street address, city, county, precinct, zip code
- Any and all dates (except the year) including birth date, encounter date, and date of death
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security number
- Medical record numbers
- Health plan beneficiary numbers and other identifying information
- Account numbers
- Certificate of license numbers
- Vehicle identifiers and serial numbers to include license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Full face photographic images and other comparable images
- Any other unique identifying number, characteristic or codes

Any questions about whether information is de-identified should be directed to the Privacy Officer before it is used or disclosed as non-protected information.

C. Fundraising and Marketing

Except for very limited circumstances, the use or disclosure of protected health information by Business Support Component for marketing or fundraising purposes requires an individual authorization in advance of such use or disclosure. Therefore, it is the policy of Business Support Group not to use protected health information for any marketing or fundraising purpose.

D. Disclosures to and from Business Associates

Business Support Component will only provide protected health information to a business associate if a Business Associate Agreement is signed by the business associate ensuring that any protected health information is protected. The term "business associate" is defined in the Policy on Compliance with HIPAA Privacy Regulations as:

Persons or entities that provide services or assist the covered entity in the performance of an activity or function involving the use of protected health information or other regulated activities.

Examples of Business Associates include vendors, lawyers, accountants, and business service companies that need protected health information to perform a function for the Business Support Component. All staff members must report to the Privacy Liaison any third parties who receive protected health information from that staff member or from Business Support Component. The name of the company or individual, the contact person, the address, and the reason for the disclosures shall be provided to the Privacy Liaison who will forward the information to the appropriate individual at University Contracting who will assist in obtaining the agreement in the appropriate format.

6. Individual's Rights

A. Restrictions in Disclosure Authorization

Individuals have the right to ask that the use and disclosure of the individual's protected health information be limited. It is the policy of Business Support Component to refer any such requests it receives directly to the Privacy Officer for consideration and response. If the Privacy Officer notifies Business Support Component that a restriction has been accepted that will affect Business Support Component's use or disclosure of the protected health information, Business Support Component is obligated to comply with the restriction, and must therefore ensure that all appropriate measures are taken to comply with any agreed restriction. Business Support Component will cooperate with the Privacy Officer or his designee in determining whether a requested restriction(s) can be tracked and enforced. If Business Support Component cannot comply with the requested restriction, it shall immediately notify the Privacy Officer.

B. Access by patients or employees

Individuals have the right to access their own protected health information, and any requests received by a staff member shall be reviewed and a response provided to the individual within 30 days of the request. In certain situations, the request may be denied. If it is, the individual will be notified in writing, the reasons for the denial and the individual's right to have the denial reviewed.

C. Right to Amend

Individuals have the right to request an amendment to their protected health information, and any requests received by a staff member shall be provided to the Privacy Liaison. The Privacy Liaison will work cooperatively with the Privacy Officer to accommodate any such requests in a timely manner.

D. Accounting of Disclosures

Individuals have the right to obtain an accounting of all disclosures of their protected health information after April 14, 2003, except for the following disclosures: treatment, payment and healthcare operations; disclosures to the individual or authorized by the individual; disclosures in a limited data set, and disclosures to person's involved in the individual's care. Business Support Group must track any disclosures of protected health information not exempted from the accounting requirement. The accounting must include all other disclosures, including specifically disclosures that are:

1. Required by law
2. Required for public health activities
3. For health oversight activities
4. Reports of abuse
5. For judicial and administrative proceedings (i.e., Subpoenas, court orders, etc.)
6. For law enforcement purposes
7. To the coroner
8. For research (except where authorized or pursuant to a Limited Data Set Agreement)
9. Necessary to avert a threat of serious injury
10. Unlawful or unauthorized disclosures

All such disclosures must be tracked and retained by the Privacy Liaison for a period of six years. This written account is to include:

1. The date of release.
2. Name of person or entity and address who received the information.
3. A brief description of the information released.
4. A statement of the purpose for the information, or, instead of a statement, a copy of the written request for the information.

The Privacy Liaison will forward any requests for an accounting received by Business Support Group to the Privacy Officer. The Privacy Liaison shall submit with the request all information it has retained about disclosures by Business Support Group that are subject to the accounting requirement.