

HIPAA LIAISON EXPECTATIONS

The following document describes the expectations for the role of HIPAA Liaison in each of the covered entities at Purdue University. The responsibilities of this role will change as new compliance requirements are defined; however, the liaison role will remain a critical component of Purdue's overall implementation of procedures for compliance with the regulations. Although the development and implementation of HIPAA training materials and University-wide HIPAA Policies and Procedures, the primary contact for privacy complaints and general HIPAA information is the responsibility of The Office of Legal Counsel, ultimately, compliance with all applicable laws and with University policies and procedures is the responsibility of the individual departments and the HIPAA Liaison is the primary contact for the departmental compliance effort.

Background

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a federal law passed by Congress in 1996 and is part of the Social Security Administration Act. The law includes a trio of HIPAA regulations designed to protect and standardize the transmission of healthcare information with which providers will be required to comply.

In December of 2000, the United States Department of Health and Human Services released privacy regulations implementing HIPAA's requirements. The final HIPAA privacy regulations became effective on April 14, 2001 and most covered entities were to be in compliance with the regulations by April 14, 2003. In March 2002, HHS released proposed revisions to the regulations, and these new rules became final in August 2002. On February 17, 2009, as part of the stimulus bill, President Obama signed the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). The HITECH Act significantly expanded the Health Insurance Portability and Accountability Act's ("HIPAA") privacy and security requirements. Also, on March 26, 2013, the Omnibus bill was passed which finalized interim provisions in HITECH and added requirements to the Privacy, Security Rules, Enforcement and Breach provisions, as well as modifications to GINA.

The privacy standards apply to the following entities: 1) health plans; 2) healthcare clearinghouses; 3) healthcare providers who conduct certain electronic transactions and 4) business associates who provide business functions on behalf of covered healthcare providers or covered health plans and their subcontractors. Those providers or entities who use outside billing companies to submit billing and claims information electronically on their behalf are considered to be transmitting health information electronically and are therefore covered under the privacy standards. Therefore, "covered entities" include hospitals, skilled nursing facilities, physician practices and most other healthcare providers. Entities such as Purdue may also be covered entities, even if the entity's primary purpose is not the provision of healthcare services, if the entity has a unit, which is a health plan, healthcare clearinghouse or healthcare provider. Such entities are referred to as "hybrid entities" under the regulation.

Additionally, protected health information that is held or transmitted electronically by a covered component, must be safeguarded in compliance with the HIPAA Security Rule. The Security Rule, compliance date April 20, 2005, specifies administrative, physical, and technical safeguards that must be in place to secure protected health information as required and as identified as reasonable and appropriate given the outcome of the entity's risk assessment.

Finally, the Transactions and Code Sets Standards, effective October 16, 2002, were implemented to require that certain electronic transactions that include protected health information (e.g. billing), would be formatted according to a standard and that standard code sets were used. This law was intended to increase the efficiency of transaction processing in the health care industry.

In the case of both the HIPAA Privacy and Security Rules, compliance must be properly documented and maintained for 6 years.

Declaration of Hybrid Entity Status and Designation of Covered Components

Purdue University endeavors to preserve the privacy and confidentiality of the protected health information and medical records maintained by its various schools and departments. It strives to fulfill this responsibility in accordance with state and federal statutes and regulations. Further, Purdue acknowledges its general obligations of trust and confidentiality reposed in its employees and students who are responsible for medical or mental health treatment at the University. As a hybrid entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Purdue will ensure that its designated "covered components" comply fully with the requirements of 45 C.F.R. Parts 160, 164, which are the HIPAA Privacy Regulations.

Purdue University is a hybrid entity under the HIPAA Privacy Regulations. Purdue's primary purpose is education; however, Purdue does have departments and covered components that provide covered healthcare services, and Purdue has self-insured health plans. Purdue also has offices or departments that provide business support to the healthcare provider and health plan covered components, and these business support offices or departments have or may have access to protected medical and health information. Purdue also acts as a business associate to external covered entities. Purdue University, therefore, has surveyed its departments to identify and designate its covered components. The up-to-date list of designated covered components can be found at: <https://www.purdue.edu/legalcounsel/HIPAA/Covered%20Comp.html>.

Liaison Responsibilities

A liaison has been designated for each of the covered components. The role of the liaison includes the following responsibilities relating to the assigned covered component(s):

- Maintain an ongoing and accurate list of staff who are designated as covered by HIPAA, in the covered components for which you are responsible. Maintain this history for 6 years.
- Maintain documented procedures for implementing the HIPAA regulations and ensure that these procedures are being followed in your designated area(s).

- Communicate policies and procedures relating to HIPAA compliance to all employees. Also, communicate changes to the policies or procedures to affected employees as they occur. Identify, develop and distribute area-specific policies and procedures, with input from the HIPAA Privacy and Security Officers, as needed.
- Ensure that new covered employees complete HIPAA training upon hire and all covered employees review HIPAA training annually. Provide a list annually of workforce that have completed HIPAA training in the previous calendar year, to The Office of Legal Counsel, when requested.
- Forward HIPAA Privacy complaints to The Office of Legal Counsel and HIPAA Security Complaints to the HIPAA Security Officer. Assist with the investigation of complaints issued by patients/employees, following the HIPAA Complaint Procedures.
- Ensure that inadvertent disclosures of PHI are documented, investigated and quickly forwarded to The Office of Legal Counsel.
- Ensure that security incidents are reported according to the University Incident Response Policy.
- Work with The Office of Legal Counsel to ensure that breach notifications to individuals are developed and sent, as required.
- Maintain all HIPAA documentation related to your area (ie. Confidentiality agreements, authorizations, covered workforce lists) for 6 years upon the date of creation or effective date, whichever is later.
- Attend the HIPAA Liaison Committee meetings, communicating HIPAA-related issues affecting your area.
- Act as the primary point of contact for questions, audits, assessments, policy review and problem resolution regarding HIPAA compliance issues.
- Participate in HIPAA privacy and security reviews, conducted by The Office of Legal Counsel and/or ITaP Security and Policy or their delegates.
- Ensure that the HIPAA Security Officer is contacted by IT staff to ensure that new functionality or systems impacting electronic PHI is configured securely.
- On an ongoing basis, identify business associates and communicate the need for business associate agreements to The Office of Legal Counsel.
- Ensure that HIPAA liaison duties are administered by other staff when the liaison is out for extended periods.
- Ensure that HIPAA authorizations received in other than Purdue's standard format, are sent to The Office of Legal Counsel for approval, prior to releasing the requested information.

- For covered healthcare providers and health plans, ensure that the distribution of the Notice of Privacy Practices is occurring, according to the HIPAA Privacy Rule requirements.
- Ensure that rights of the individuals, e.g. requests for amendment, restriction requests, request for confidential communication.

The role of the liaison is of utmost importance in ensuring that the HIPAA regulations are communicated and followed in each of the covered components at Purdue. Good communication and coordination with The Office of Legal Counsel is necessary to ensure that the area procedures are up-to-date with changes in the regulations and that issues and questions are resolved expeditiously.

For help with HIPAA questions, please contact:

The Office of Legal Counsel
610 Purdue Mall
West Lafayette, IN 47907-2052
Email: legalcounsel@purdue.edu

I understand my responsibilities regarding compliance with HIPAA, listed above, for the areas that are assigned to me as HIPAA Liaison.

HIPAA Liaison Signature

Date

HIPAA Liaison Printed Name