HIPAA Breach Notification Policy

Final breach notification regulations, effective for breaches discovered on or after September 23, 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act and finalized by the Omnibus Bill, effective March 23, 2013, by requiring HIPAA covered components and their business associates to provide notification following a breach of unsecured protected health information.

The regulations, developed by the Office for Civil Rights, require HIPAA covered components to promptly notify affected individuals of a breach of their protected health information, as well as the Health and Human Services (HHS) Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered components to notify the covered component of breaches at or by the business associate or its workforce, agents or subcontractors.

It is the policy of Purdue University to comply with these regulations and, therefore, the following procedures have been implemented to assure compliance.

Steps for Notifying HIPAA Administration

The following procedures are in place for reporting uses and disclosures in violation of the HIPAA Privacy Rule to the Office of Legal Counsel, by Purdue's covered components or business associates.

- The inadvertent disclosure tracking process (form at: https://www.purdue.edu/legalcounsel/HIPAA/recordofinadvertentdisclosureofprotectedhealthinformation.pdf) includes the requirement to provide a copy of the Inadvertent Disclosure form to the Office of Legal Counsel.
- Regarding the reporting of security incidents to ITaP Security and Policy (ITSP), where the incident includes the potential access of protected health information, ITSP will notify the Office of Legal Counsel and Security Officers (Incident Response Policy: https://www.purdue.edu/policies/information-technology/s17.html).
- Also, business associates of Purdue's covered components are required by the Business Associate Agreement, to notify Purdue of any unauthorized use or disclosure by the business associate or its workforce, agents or subcontractors that violates the HIPAA Privacy or Security Rules and the remedial action taken or proposed to be taken with respect to the use or disclosure. The Office of Legal Counsel and Security Officers will be contacted for issues pertaining to the potential access of electronic PHI, other inappropriate uses or disclosures of PHI will be reported to the Office of Legal Counsel.

Timeliness

A breach shall be treated as discovered by a covered entity, business associate or its subcontractor, as of the first day on which such breach is known or should reasonably have been known to the covered entity, business associate or its subcontractor, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach, as defined in the rule. This discovery is triggered as soon as any person, other than the individual committing the breach, who is an employee, officer, or other agent of the covered entity, business associate or its subcontractor, knows or should reasonably have known of the breach.

Purdue will make the individual notifications as soon as reasonably possible after the covered entity takes a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual. Notifications to individuals must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach, except when law enforcement requests a delay. Purdue may provide the required information to individuals within the required time period in multiple mailings as the information becomes available.

Notification of Individuals

The Office of Legal Counsel or Security Officer, as appropriate, given the type of breach involved, will work with University counsel to determine whether a breach has occurred and what notification requirements may be required for a particular breach.

The covered component who owns the data will be responsible to ensure that the required reporting to individuals occurs, with assistance from the Office of Legal Counsel for privacy breaches and both the Office of Legal Counsel and Security Officer for security breaches. Reports to Health and Human Services will be made by the Office of Legal Counsel.