PURDUE UNIVERSITY®

HIPAA Compliance At Purdue

HIPAA INADVERTENT DISCLOSURE PROCEDURES

The Health Insurance Portability and Accountability Act of 1996 requires that HIPAA covered components report and track incidents that may result in disclosures of Protected Health Information (PHI) in violation of the HIPAA Privacy or Security Rules. Some of these disclosures may be breaches that will be addressed in accordance with Purdue's HIPAA Breach Notification Policy and Procedures.

Steps for Notifying HIPAA Administration of a Potential Disclosure of PHI:

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

An inadvertent disclosure is defined as a use or disclosure which violates the HIPAA Privacy and/or Security Rules or violates HIPAA's minimum necessary requirements.

1. Notice that an inadvertent disclosure has occurred is made to the affected area HIPAA Liaison by the person who disclosed or discovered the disclosure. The list of University HIPAA Liaisons can be viewed at: https://www.purdue.edu/legalcounsel/HIPAA%20forms%202020/liaison%20roster%200723201.pdf. The forms used to process the Inadvertent Disclosure can be located at: https://www.purdue.edu/legalcounsel/HIPAA/FormsProcedures.html.
2. The Record of Inadvertent Disclosure of PHI – Form must be filled out by either the person who inadvertently disclosed the information or by the HIPAA Liaison when reported by a person who discovered that a disclosure occurred, but the person who disclosed the PHI is unknown. This should happen immediately and at least within one business day of discovery.
3. The HIPAA Liaison will investigate, ensure that the details about the possible disclosure and how the event occurred are recorded on the form and that the issue is mitigated (e.g. confidentiality agreement and/or destruction certificates are obtained from the recipient). Immediately upon notification of an inadvertent disclosure, the HIPAA Liaison will contact the recipient and request that the Inadvertent Disclosure Confidentiality Agreement is signed. If the recipient returns the information, this is all that is required. If the recipient is remote and requests to destroy the information, the Inadvertent Disclosure Disposal Verification is also requested from the recipient to document secure disclosure of the information. If the recipient notifies Purdue in person, the staff person receiving the report should attempt to obtain signature on the confidentiality agreement.
4. The forms are submitted to the Office of Legal Counsel to complete a risk assessment to determine whether a reportable breach has occurred. A copy of the information disclosed should be provided with the form, if possible, and confidentiality agreements and destruction certificate as they are received. If the confidentiality agreement and destruction certificate are not returned within one business day of receipt of the disclosure document,

the document should be submitted to the Office of Legal Counsel to begin the risk assessment and to comply with the notification requirements, as necessary. If a potential violation of the HIPAA Security Rule has occurred, the Office of Legal Counsel will alert the HIPAA Security Officer and a parallel investigation will occur.

5. Breaches are addressed in accordance with the HIPAA Breach Notification Policy, https://www.purdue.edu/legalcounsel/HIPAA%20forms%202020/breachnotificationpolicy-20201.pdf. The HIPAA Liaison will be responsible for providing the contact names and addresses to the Office of Legal Counsel for provision of individual notification letters. For larger breaches, the department may be required to process the notifications and will be responsible for any costs incurred as a result of the breach.
6. The incident history is also reviewed to identify whether the employee has had other recent incidents and a discussion will occur, as necessary, between the Office of Legal Counsel and Department Head and/or Supervisor to determine whether any disciplinary action is warranted. Whether a breach has occurred does not necessarily dictate whether there should be disciplinary follow up on the incident.