HIPAA Breach Notification Procedures

The Health Insurance Portability and Accountability Act of 1996 requires that HIPAA covered components, their business associates and business associates' contractors, provide notification following a breach of ***unsecured*** protected health information.

The regulations, 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 affected individuals without unreasonable delay and to HHS Secretary on an annual basis. The regulations also require business associates of covered components and their subcontractors to notify the covered component of breaches of its PHI.

Steps for Notifying HIPAA Administration

The following procedures are in place for reporting uses and disclosures in violation of the HIPAA Privacy or Security Rules to the HIPAA Privacy and/or Security Officer, by Purdue's covered components, business associates, or their subcontractors.

- 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 HIPAA Privacy Officer.
- 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 HIPAA Privacy 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 HIPAA Privacy 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 HIPAA Privacy Officer.

Breaches Reported by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate or its subcontractor, the business associate must notify Purdue's HIPAA Privacy Officer (for potential privacy breaches) or Purdue's HIPAA Security Officer (for potential security breaches) following the discovery of the breach. A business associate must provide notice to Purdue without unreasonable delay and no later than 24 hours from the discovery of the breach. To the extent possible, the business associate should provide the HIPAA Officer with the identification of each

individual affected by the breach as well as any information required to be provided by Purdue in its notification to affected individuals. Also, provided by the business associate is a description of the cause and action plan for preventing reoccurrence. If the breach was discovered by the business associate's subcontractor, the subcontractor will notify and provide the pertinent information to the business associate and the business associate will then, provide notification to Purdue.

With respect to timing, if a business associate is acting as an agent of Purdue then, the business associate's discovery of the breach will be communicated to Purdue at the time of discovery. In such circumstances, Purdue must provide notifications based on the time the business associate discovers the breach, not from the time the business associate notifies Purdue. In contrast, if the business associate is not an agent of Purdue, then Purdue is required to provide notification based on the time the business associate notifies Purdue of the breach.

Identification of a Breach

Breaches can include protected health information in any form or medium, including electronic, paper, or oral. When the HIPAA Privacy Officer receives a report of an inappropriate use or disclosure, the Privacy Officer will conduct a risk assessment to determine whether a reportable breach has occurred and then work together with University counsel to determine the appropriate reporting requirements.

In the case of a security incident, the HIPAA Privacy and Security Officers will be notified, a risk assessment will be completed by the Privacy Officer with input from the Security Officer to determine whether a HIPAA breach has occurred and then the Security Officer will work with University Counsel to determine the HIPAA and other legal implications of the incident. If the incident has been determined to be a HIPAA breach, the Privacy Officer will coordinate with the department who owns the data and the HIPAA Security Officer to accumulate the information necessary for reporting.

Once a potential breach has been reported to the HIPAA Privacy or Security Officer, the following ***assessment*** will be conducted to determine whether the incident is reportable. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised or one of the other exceptions to the definition of breach applies.

- ✓ Did the potential breach occur on or after September 23, 2009?
- ✓ Was the protected health information secured (encrypted or rendered unusable, unreadable or indecipherable to unauthorized individuals)?
- ✓ Did the use or disclosure of protected health information violate the HIPAA Privacy Rule (including disclosures of more than the minimum information necessary for the intended purpose.)?

- ✓ Does the use or disclosure fall under one of the following exceptions to the notification requirement?

  The potential breach was an:

  - unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity, business associate or their subcontractor (if the act was by an individual acting under the authority of a covered entity or a business associate, in good faith, within the course and scope of employment or professional relationship) and did not result in further use or disclosure.
  - inadvertent disclosure of protected health information from one person to another person, both authorized to access protected health information at a covered entity, business associate or their subcontractor, at the same facility if the information was not further used or disclosed without authorization. For example, to person's working onsite that are not workforce members, such as physicians with staff privileges.
  - unauthorized disclosure in which the covered entity had a good faith belief that an unauthorized person to whom protected health information was disclosed would not have been able to retain the information (e.g. mailings sent to the wrong individual that are returned as undeliverable, a nurse hands discharge papers for one patient to another patient but retrieves the papers prior to the patient having a chance to read or retain what they saw).

- ✓ Is there a low probability that the protected health information has been compromised, based on a risk assessment that considers at least the following factors:

  - the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; For example, Was the information involved sensitive in nature? If there were few identifiers, what is the probability that the information could be re-identified?
  - the unauthorized person who used the protected health information or to whom the disclosure was made. For example, is the recipient obligated to protect the privacy and security of the information?
  - whether the protected health information was actually acquired or viewed (or only the opportunity existed to acquire or view the information).
  - the extent to which the risk to the protected health information has been mitigated. For example, were satisfactory assurances obtained from the recipient that the information will not be further used or disclosed (e.g. confidentiality agreement) or will be destroyed (e.g. with a destruction certificate).

Notification of Individuals

The HIPAA Privacy 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 HIPAA Privacy Officer for privacy breaches and both Privacy and Security Officers for security breaches. Reports to Health and Human Services will be made and documented by the HIPAA Privacy Officer.

Methods of Notice

Purdue will provide breach notice to the individual in written form by first-class mail at the last known address of the individual.

Where the individual affected by a breach is a ***minor*** (a person under the age of 18) or otherwise lacks legal capacity due to a physical or mental condition, notice will be provided to the parent or other person who is the personal representative (e.g. power of attorney or guardian) of the individual.

If the individual is known to be ***deceased***, notice will be sent to the last known address of the next of kin or personal representative, if this contact information is known and up-to-date.

Substitute Notice

If Purdue does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, Purdue will provide substitute notice for the unreachable individuals. The substitute form of notice will be reasonably calculated to reach the individuals for whom it is being provided.

If there are ***fewer than 10 individuals*** for whom Purdue has insufficient or out-of-date contact information to provide the written notice, Purdue will provide substitute notice to such individuals through an alternative form of written notice, by telephone, or other means, such as posting a notice on Purdue's web site.

If Purdue has insufficient or out-of-date contact information for ***10 or more individuals***, then Purdue will provide substitute notice through either a conspicuous posting for a period of 90 days on Purdue's home page or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. Purdue will provide a toll-free phone number in the notice, active for 90 days, where an individual can learn whether their unsecured protected health information may be included in the breach.

If Purdue uses a hyperlink on the home page to convey the substitute notice, the hyperlink will be prominent so that it is noticeable given its size, color, and graphic treatment in relation to other parts of the page, and it will be worded to convey the nature and importance of the information to which it leads.

Content of the Notice

In addition to HIPAA breach notification, if other notifications or actions are required, such as those associated with social security numbers or where GLBA red flag procedures apply, the HIPAA Privacy and Security Officers and University counsel will coordinate actions to be taken. The HIPAA breach notification will include, to the extent possible, the following elements:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved). Covered entities should not include a listing of the actual protected health information that was breached and should avoid including any sensitive information in the notification itself (e.g. SSN or credit card numbers);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the covered entity involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, Web site, or postal address.

Purdue is permitted to send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, so long as they all reside at a single address and the covered entity clearly identifies on the notice the individuals to which the notice applies. Further, where a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, a covered entity must address a breach notice to the dependent himself or herself.

Health Information Organizations

Similarly, when multiple covered entities participate in electronic health information exchange and there is a breach of unsecured protected health information at a Health Information Organization (HIO), the obligation to notify individuals of the breach falls to the covered entities. In such circumstances, it may be necessary for the HIO to notify all potentially affected covered entities and for those covered entities to delegate to the HIO the responsibility of sending the required notifications to the affected individuals. This would avoid the confusion of individuals receiving more than one notification about the same breach.

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.

Law Enforcement Delay

A temporary delay of notification is required in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required. In such instances, Purdue is required to delay the notification, notice, or posting for the time period specified by the official.

Also Purdue is required to temporarily delay a notification, notice, or posting if a law enforcement official states orally that a notification would impede a criminal investigation or cause damage to national security. However, in this case, Purdue must document the statement and the identity of the official and delay notification for no longer than 30 days, unless a written statement meeting the above requirements is provided during that time.

Media Notice

If Purdue experiences a breach affecting more than 500 residents of a State or jurisdiction, in addition to notifying the affected individuals, will provide notice to prominent media outlets serving the State or jurisdiction. Purdue will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and will include the same information required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), Purdue will notify the Secretary of breaches of unsecured protected health information. The Secretary will be notified by Purdue of breaches using the HHS web site, filling out and electronically submitting a breach report form (form at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html).

If a breach affects 500 or more individuals, Purdue will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

For breaches of unsecured protected health information involving less than 500 individuals, The HIPAA Privacy Officer will maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for breaches discovered during the preceding calendar year, not occurred in the previous calendar year, in the manner specified on the HHS web site.

Follow Up with a Business Associate

When a breach has been reported by a business associate, the HIPAA Privacy or Security Officer, as appropriate, will obtain from the business associate a written description of the cause of the breach and action plan for preventing reoccurrence. The HIPAA Privacy Officer, for privacy breaches or the HIPAA Security Officer for security breaches, will follow up with the business associate to receive assurances that the action plan has been completed by either the business associate or its contractor, depending on where the breach occurred. The follow up will be documented and included with the incident documentation.

Definitions

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable,

demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Personal representative of a deceased individual is a person who has authority to act on behalf of the decedent or the decedent's estate.

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.