Health Insurance Portability and Accountability Act of 1996

Compliance at Purdue

https://www.purdue.edu/legalcounsel/HIPAA/index.html

legalcounsel@purdue.edu

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Federal law
  - Part of the Social Security Administration Act
- Protects the *confidentiality and security of personally identifiable health information* as it is used, disclosed and electronically transmitted by covered entities
- Creates framework, using standardized formats, for transmitting electronic health information more cost effective

All departments and workforce designated by Purdue's HIPAA Privacy Officer as HIPAA covered components MUST comply with its requirements.

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html

legalcounsel@purdue.edu

What is Protected Health Information (PHI)?

- The Privacy Rule protects all *individually identifiable health information* held or transmitted by a covered entity, its business associates or a business associate's subcontractors, in any form or media.
  - This information is also known as *Protected Health Information (PHI).*
  - Includes information tied to a covered health care provider or health
- PHI includes:
  - Demographic data
  - Individual's past, present or future physical or mental health conditions
  - The provision of health care to the individual
  - Past, present, or future payment for the provision of health care to the individual
  - Information that identifies or can be used to identify the individual

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html

legalcounsel@purdue.edu

PHI

- Some examples of protected health information at Purdue includes:
  - Prescription information processed by Purdue University Pharmacy
  - Health claims processed by Purdue's health plan administrators
  - Clinic billing information processed by the Accounts Receivable department
  - Treatment or accounts receivable information accessed by ITaP
- Information excluded from the definition of PHI:
  - *Employment records*
  - *Education records*
  - *Health information about individuals who have been deceased for more than 50 years*
  - *De-identified information* which must have the subject's name, email address, telephone numbers, or any other information that could be used alone or in combination to identify the subject removed
    - The Office for Civil Rights provides further guidance regarding de-identification at: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

HIPAA Legal Overview

- The Privacy Rule (2003)
  - Applies to covered entities and provides safeguards to protect PHI
  - Identifies *permitted uses and disclosures, rights of individual* to control how their PHI is used and disclosed, establishes *administrative requirements*, and *application of sanctions*
- The Security Rule (2005)
  - Protects the confidentiality, integrity and availability of *PHI that is maintained or transmitted electronically*
  - Requires *administrative, physical and technical safeguards* to protect PHI, safeguards must be *addressable* (can address its applicability for a particular environment) and requires a *sanction policy*
- HITECH (2010)
  - Expands HIPAA Privacy Requirements to directly cover *business associates*, who are now required to report to covered entities
- Omnibus Rule (2013)
  - New regulations affecting The Privacy Rule, Security Rule, HITECH
  - Implemented new regulations such as Genetic Information Nondiscrimination Act (GINA), *breach notifications*, *marketing*, *fundraising*, *school immunization records*, *research authorizations* and *enforcement*

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html

legalcounsel@purdue.edu

Penalties for Non-compliance

- Secretary of Health and Human Services (HHS) has authority to impose penalties to non-complying entities.
- HITECH Act (2010) requires HHS to develop procedures by which an individual harmed by a HIPAA breach of PHI may obtain a percentage of the HHS enforcement penalties.
- The *covered entity and specific individuals* can be investigated and prosecuted with *Civil, State, and Federal Criminal penalties*
  - Fines can reach up to $250,000 and 10 years of imprisonment per violation

Who is Covered by HIPAA?

- *Health care providers* who transmit PHI in electronic form in connection with certain electronic transactions defined by federal regulations (e.g. electronic billing and remission of payments electronically)
- *Health care clearinghouses*
- Certain *health plans*
- *HIPAA business associate* which is a person or organization that performs certain business functions on behalf of the covered entity and involves the use, maintenance, or disclosure of PHI
  - Prior to disclosing PHI to a business associate, covered entities are required to enter into a written agreement that imposes safeguards

If your department is covered by HIPAA, is planning to disclose PHI to an outside entity, and you are unsure about whether an agreement is required, ask your HIPAA liaison to contact the HIPAA Privacy Officer (x66846) PRIOR to disclosing any PHI!

How does HIPAA impact Purdue?

- Purdue University is designated as a *hybrid entity*
  - All of Purdue is NOT covered by HIPAA - only *those areas that have been formally designated as covered components* by the HIPAA Privacy Officer.
- Covered components include:
  - Purdue Student Health Center, Purdue University Pharmacy, Purdue's North Central Nursing Clinic, Employee Wellness Programs, Student and Receivables Business Services-Accounts Receivable, ITaP, Bursar, and others
- A full list of departments at Purdue that are covered by HIPAA can be found at: https://www.purdue.edu/legalcounsel/HIPAA/Covered%20Comp.html

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html
legalcounsel@purdue.edu

Covered Components' Responsibilities

- Name a *HIPAA Privacy Liaison* who will be responsible for communicating HIPAA policies and procedures, ensuring that training occurs, maintaining documentation for 6 years, and discussing with the HIPAA privacy compliance director any new issues.
- Determine and document *which staff are included* in the covered component and *determine which roles need access to PHI.*
- Ensure that *all HIPAA policies and procedures are followed* and *apply sanctions.*
- Identify *business associates.*
- Ensure that *privacy and security safeguards are in place and followed.*

Staff Responsibilities within a Covered Component

- Complete HIPAA training upon hire and then annually thereafter
- Read the *Notice of Privacy Practices (NPP)* applicably to the area in which they work
  - NPP is a document which is distributed to individuals who receive services *from Purdue's HIPAA-covered health care providers and health plan components.*
  - NPP describes *how PHI may be used and disclosed by Purdue's covered components* and the *rights of an individual* to control how their information is used and disclosed.
- Know how HIPAA regulations impact the employee's individual job procedures
- Agree to comply with the official confidentiality agreement
- Ensure compliance with the "*minimum necessary*" rule

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html
legalcounsel@purdue.edu

Minimum Necessary

- HIPAA requires that uses, disclosures, and requests of PHI must be limited to *the minimum necessary information needed to accomplish the intended purpose.*
- Minimum necessary does NOT apply to:
  - Disclosures to or requests by a health care provider for treatment purposes
  - Uses or disclosures made to the individual
  - Uses or disclosures pursuant to an authorization
  - Uses or disclosures to Health and Human Services
  - Uses or disclosures that are required by law or required for compliance with the HIPAA privacy rule

Only workforce members with responsibilities related to a particular patient or health plan member may access information pertaining to that individual and only the minimum necessary information should be accessed to perform the related work responsibilities!

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html
legalcounsel@purdue.edu

HIPAA Authorizations

- HIPAA requires that a valid HIPAA authorization be obtained from an individual or their representative before sharing information for the following purposes:
  - Disclosures of psychotherapy notes
  - Marketing
  - Disclosures that constitute a sale of PHI
  - Any other use or disclosure inside or outside of the covered component other than for purposes exempted by HIPAA
- Purdue's HIPAA authorization form should be used when an authorization is obtained from a patient by Purdue's covered components
  - If HIPAA authorization is not received on Purdue's approved form, the authorization must be reviewed by the HIPAA Privacy Officer PRIOR to disclosure of PHI.

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html
legalcounsel@purdue.edu

Using and Disclosing PHI

- PHI should only be used and disclosed without a written HIPAA authorization for:
  - *Treatment*
  - *Payment of health care services*
  - *Health care operations*
  - Instances *authorized by the patient*
  - *Other circumstances described in the Privacy Rule* (e.g. public health and as required by law)
- Use means the sharing, employment, application, utilization, examination, or analysis of PHI, within an entity that maintains such information.
- Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

If treatment information is requested from an outside provider on a non-emergency basis and it is unknown whether they legitimately have a treatment relationship with the patient, an authorization should be obtained from the patient PRIOR to sharing PHI!

Disclosure to Family, Friends, and Others Who are Involved in Patient Care or Payment

- Health care providers may disclose PHI to:
  - *Any person identified by the individual*, however, the PHI must be directly related to that persons' involvement in the individual's care or payment for that care.
  - Notify a person *who is responsible for the care of the individual* or the individual's location or general health.
- PHI may be disclosed for this purpose, under these conditions:
  - If you have *asked the individual if it is okay* to disclose PHI prior to the disclosure, given the individual an *opportunity to object*, or you can *reasonably infer* from the circumstances, based on professional judgement, that the individual does not object
  - If the individual is not present, you *may use your professional judgement* in determine that it is in the best interest of the individual to disclose PHI directly relevant to a person's involvement in the individual's care or payment for care

Please review the HIPAA Communication Guidelines, and the guidelines addressing Disclosures to Family, Friends, and Others at https://www.purdue.edu/legalcounsel/HIPAA/Guidelines.html

Individual's Access to PHI

- Individuals have the right to inspect, access, or obtain copies of their own PHI.
  - A written request for the record must be obtained to document the disclosure.
- A covered component may deny an individual access, without providing the individual an opportunity for review, in the following circumstances:
  - *Psychotherapy notes*
  - Information compiled in a reasonable anticipation of, or *for use in a civil, criminal, or administrative action or proceeding*
  - An individual's access to PHI *created or obtained by a covered health care provider in the course of research* that includes treatment while the research is in progress
  - If the *PHI was obtained by someone other than a health care provider under a promise of confidentiality* and access will reveal the source of information

Individual's Access to PHI

- Reviewable grounds for denial include:
  - Release of information is reasonably likely to *endanger the life or physical safety* of the individual or another person.
  - PHI makes *reference to another person.*
  - The *provision of access to the individual's personal representative is likely to cause substantial harm* ,as deemed by a licensed health care professional, to the individual or another person.
- If access is denied and the grounds are reviewable, the *individual has the right to request review* by a licensed health care professional who is designated by the covered component to act as a review official.
- The covered entity must *act on a request for access no later than 30 days* after the receipt of the request.

Research and HIPAA

- Research is not considered part of treatment, payment or healthcare operations. Therefore, use of PHI for research purposes is limited.
- In general, any PHI intended for research purposes must:
  - Be obtained through documented release (HIPAA authorization) by the study participant.
  - Be fully described and approved in an Institutional Review Board (IRB) protocol.
  - Comply with information security requirements.
- Exceptions exist for this requirement, but must be obtained with explicit approval from the Covered Entity's Privacy Board and/or an IRB.

Examples of Research Activities Excepted from HIPAA Authorization

- Waiver of HIPAA Authorization
- Reviews preparatory to research by staff of the covered entity
- Research involving a decedent's information
- Use of a Limited Data Set
- Full De-identification

- Source https://privacyruleandresearch.nih.gov/pr_08.asp

Waiver of HIPAA Authorization for Research Purposes

- Researchers must satisfy these IRB criteria:
  - The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals based upon the presence of the following elements:
    - An adequate plan exists to protect the identifiers from disclosure or improper use;
    - An adequate plan exists to destroy the identifiers at the earliest opportunity practical under the research, unless there is a health or research justification for retaining the identifiers or the retention is otherwise required by law; and
    - Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except required by law, authorized oversight of the research project, or for other research conducted consistent with the requirements of the Privacy Rule.
  - The research could not practicably be conducted without the waiver or alteration to the authorization; and
  - The research could not practicably be conducted without access to and use of the PHI

- *Note that a waiver of HIPAA Authorization ***differs*** from a waiver of informed consent to participate in research and if needed is addressed by an IRB separately.

Reviews Preparatory to Research

- When a researcher is part of the workforce of a covered entity, the covered entity may allow a researcher access to PHI for recruitment of potential participants in a study when a researcher makes oral or written representation that the use or disclosure of the PHI is:
  1. solely to prepare a research protocol or similar purposes preparatory to research,
  2. the researcher will not remove the PHI from the premises, and
  3. the use or disclosure is necessary for research purposes.
- A researcher who is not part of the covered entity's workforce, cannot have access to PHI without patient authorization or unless the researcher has obtained a waiver from the IRB to permit this access for recruitment purposes.

Research on Decedents

- The PHI associated with a deceased person may be used or disclosed for research purposes ***without*** an authorization. A covered entity may rely on a researcher's oral or written representation that:
  - the use or disclosure of the PHI is solely for research on the PHI of a decedent,
  - that the PHI sought is necessary for the research, and
  - at the request of the covered entity, that documentation of the death of the affected Individuals be provided.

Fully De-Identified Data for Research

- Covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule. Covered entities seeking to release this health information must determine that the information has been de-identified using either statistical verification of de-identification or by removing certain pieces of information from each record as specified in the Rule.
- The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members; these elements are enumerated in the Privacy Rule. The covered entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information.
- *Information is considered de-identified ONLY if ALL of the following information is removed AND the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.*

Categories of Identifiers

- Name
- All geographic subdivision smaller than a state including: street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except the year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older - Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers

Categories of Identifiers (continued)

- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and other comparable images, and
- Any other unique identifying number, characteristic or code, except a code assigned to allow information de-identified to be re-identified by the covered entity, provided that:
  - The code is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
  - the covered entity does not use or disclose the code or other means of identification for any other purpose and does not disclose the mechanism for re-identification.

Limited Data Sets in Research

- A covered entity may use and disclose a Limited Data Set (LDS) for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing covered entity and the LDS recipient enter into a data use agreement.
  - Data must be free of a defined list of 16 categories of defined identifiers.
  - LDS can contain city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers.
- A covered entity may disclose a LDS for public health purposes, including those that are emergency preparedness activities. The covered entity must have a data use agreement in order to disclose the LDS.
- Data are still considered PHI under the Privacy Rule.

Data Use Agreements for Limited Data Sets in Research

- **Data Use Agreement** - An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.
- Required elements of a DUA related to PHI.
  - Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that, if done by the covered entity, would violate the Privacy Rule).
  - Identify who is permitted to use or receive the limited data set.
  - Stipulations that the recipient will
    - Not use or disclose the information other than permitted by the agreement or otherwise required by law.
    - Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the covered entity any uses or disclosures in violation of the agreement of which the recipient becomes aware.
    - Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.
    - Not identify the information or contact the individuals.
- *At Purdue University, DUAs must be signed by institutional representatives in Sponsored Program Services or Office of Legal Counsel.* Associated reviews for secure data storage and research uses are also required.

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html

legalcounsel@purdue.edu

Authorization Requirements for Marketing and Sale

- Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
  - HIPAA requires authorization for marketing purposes EXCEPT providing refill reminders or communicating about a drug/biologic that is currently prescribed for the individual or the following treatment and health care operations purposes.
  - HIPAA requires authorization for all treatment and health care operations communications where the covered component receives financial remuneration from a third party.
- Sale of PHI means a disclosure of PHI by a covered component or business associate where they directly or indirectly receive remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.
  - The authorization must state that the disclosure will result in remuneration to the covered entity.
  - Exceptions include public health, research disclosures, treatment and payment, required by law, disclosures to the individual, remuneration paid by a covered component to a business associate, use of PHI within a covered entity, disclosures of limited data sets or purposes permitted under Rule, and costs of reproducing records given to a patient.

Inadvertent Disclosures

- *Inadvertent disclosure* is a disclosure of PHI made by staff in a covered component which violates the Privacy Rule.
  - Includes impermissible uses or disclosures or disclosures that violate the minimum necessary provision

- Must be reported to the covered component's HIPAA Privacy Liaison!
  - https://www.purdue.edu/legalcounsel/HIPAA/hipaaliaisonroster.pdf
  - The liaison will ensure that the disclosure is tracked, as required, and will send a copy to the HIPAA Privacy Officer who will identify requirements to report to the individual and the Office for Civil Rights (e.g. breach reporting), if necessary.

Do NOT discuss PHI with co-workers, friends, and family or after leaving a Purdue covered component! Please do NOT share your PHI accessible accounts with others!

Breach Reporting

- There are three ways in which a breach may be identified:
  - An *inadvertent disclosure* of PHI by workforce
  - *Unencrypted electronic data* that includes PHI
  - Any *unauthorized use or disclosure* by workforce of one of Purdue's business associates, its agents, or subcontractors

- *Purdue must make notification without unreasonable delay and within 60 days* of discovery of the breach, unless a law enforcement delay has been requested.
  - Therefore, reporting to the HIPAA Privacy Officer needs to occur as soon as a potential breach is discovered.

HIPAA

https://www.purdue.edu/legalcounsel/HIPAA/index.html
legalcounsel@purdue.edu

HIPAA Liaisons and Personnel at Purdue

- A HIPAA liaison is assigned in each covered component and can be viewed at: https://www.purdue.edu/legalcounsel/HIPAA/hipaaliaisonroster.pdf

Note: Staff are prohibited form retaliating against anyone who issues a complaint.

- Questions, concerns, or complaints about the privacy policies or their implementation in your department?
  - legalcounsel@purdue.edu (HIPAA Privacy Officer)
- Contact ITaP Security and Policy if you plan to use PHI for new purposes involving computer systems, purchase of software that stores PHI, electronic transmission of PHI, or removable devices for storing accessing PHI
  - itpolicy@purdue.edu
- For general HIPAA policies, procedures, and forms at Purdue: https://www.purdue.edu/legalcounsel/HIPAA/index.html

HIPAA

Health Insurance Portability and Accountability Act of 1996

Compliance at Purdue

https://www.purdue.edu/legalcounsel/HIPAA/index.html

legalcounsel@purdue.edu

As of 2/2020