Health Insurance Portability and Accountability Act of 1996

Student Affiliation Training without Research Requirements

As of 8/1/2018
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Federal law
- Part of the Social Security Administration Act

Purpose:

☒ To protect the *confidentiality and security of personally identifiable health information* as it is used, disclosed and electronically transmitted by covered entities.

☒ It also creates a framework, using standardized formats, for transmitting electronic health information more cost effectively.
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 associates subcontractors, in any form or media, whether electronic, paper, or oral.

The Privacy Rule refers to this information as: “Protected Health Information PHI.”

PHI may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered healthcare provider or health plan, then it is PHI by definition, since it is indicative that the individual received health care services or benefits from the covered component, and therefore it must be protected in accordance with the HIPAA Rules and any business associate agreements.

PHI is information, including demographic data, that relates to:
- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies or can be used to identify the individual.
What is Protected Health Information (PHI)?

Some examples of protected health information include:

- **Treatment information** maintained by a medical or dental clinic or hospital,
- **Prescription information** processed by a pharmacy,
- **Health claims** processed by a covered health plan,
- **Clinic billing information**, processed by a clearinghouse,
- **Treatment or accounts receivable information** accessed by a software vendor while providing support for a product purchased from them by the covered entity,
- **Medical research data** gathered in preparation for disclosure to a researcher with a protocol approved by the IRB and with the appropriate HIPAA authorizations from the individual who is the subject of the data.
What is EXCLUDED from HIPAA protection?

The Privacy Rule excludes from the definition of PHI:

× employment records that a covered entity maintains solely in its capacity as an employer,

Examples: employee leave information, return to work documentation, FMLA documents, accommodation records maintained by a covered entity’s Human Resources department

× education records subject to, or defined in, the Family Educational Rights and Privacy Act (FERPA)

× Health information about individuals who have been deceased for more than 50 years.
De-identified information is not considered protected health information under HIPAA.

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.

- **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**

….more on next page
Continued…

- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- 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.
The requirements of de-identifying information are so extensive, that often the data is of limited value to researchers. The Privacy Rule permits the use and disclosure of a “limited data set” with a “data use agreement”.

To qualify as a limited data set, the following identifiers must be removed:

- Names
- Postal address information
- (other than town or city, state and zip code)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers & serial numbers, including license plate numbers
- Device identifiers & serial numbers
- Web Universal Resource Locators (URL’s)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images

The limited data set can be disclosed for purposes of research, public health, and health care operations, but the recipient must first sign the “Data Use Agreement” with the covered entity, which limits how the recipient may use the limited data set, ensures the security of the data and states that the recipient will not identify the information or use it to contact any individual.

A copy of the Data Use Agreement shall be provided to the IRB.
HIPAA's enforcement provisions authorize the Secretary of Health and Human Services (HHS) to impose penalties to non-complying entities. HHS’ Office for Civil Rights is responsible for enforcing the Privacy and Security Rules.

**Civil Penalties**

Following are the categories of violations and associated penalty amounts available.

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Such Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>$10,000-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

**Definitions:**

*Reasonable cause* means an act or omission in which a covered entity or business associate knew, or by exercising *reasonable diligence* would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

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

*Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.
Penalties for Noncompliance—Criminal

Federal Criminal Penalties
Covered entities and specified individuals, as explained below, whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations face a fine of up to $50,000, as well as imprisonment up to one year.

Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison.

Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Covered Entity and Specified Individuals
The DOJ concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

Knowingly
The DOJ interpreted the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in Violation of the HIPAA statute is not required.
State and other Penalties

The Health Information Technology for Clinical and Economic Health (HITECH) Act, gave State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules. The HITECH Act permits State Attorneys General to obtain damages on behalf of state residents or to forbid further violations of the HIPAA Privacy and Security Rules.

HHS is permitted to coordinate with other law enforcement agencies, such as the State Attorneys General or the FTC pursuing remedies under other consumer protection authorities.
The HIPAA legal requirements have evolved over several years, and include:

- The Privacy Rule
- The Security Rule
- HITECH
- Omnibus Rule (2013)
The Privacy Rule:

- applies to covered entities which must comply with the Rule. These are certain health plans, healthcare clearinghouses, certain healthcare providers and their business associates and a business associate’s subcontractors,

- provides for safeguards to protect the confidentiality of an individual’s health information,

- identifies permitted uses and disclosures,

- specifies rights of the individual to control how their health information is used and disclosed by covered components, and

- establishes administrative requirements for covered entities, including the application of sanctions to employees who violate HIPAA policies and procedures.
Compliance at Purdue

The HIPAA Security Rule:

- Was implemented to protect the confidentiality, integrity and availability of **protected health information that is maintained or transmitted electronically**.

- The Security Rule requires **administrative, physical and technical** safeguards to protect electronic PHI.

  ✓ Safeguards are either required or addressable. **Required safeguards** must be implemented as stated. **Addressable** means that the safeguard can be assessed as to its applicability for a particular environment and, if applicable, implemented as stated or an equivalent safeguard implemented, based on results of a risk assessment.

- The Security Rule **requires a sanctions policy** to discipline employees who do not follow the security policies of the covered component.

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
HITECH:

✗ Was adopted by Congress to extend HIPAA Regulations.

✗ HITECH expanded HIPAA Privacy Requirements to Business Associates (now covered directly, not just by the Business Associate Agreement).

✗ Required Breach Notification to individuals and, in some cases to Health and Human Services.

✓ Business Associates required to report to Covered Entities.
Omnibus Rule

Omnibus (effective 3/26/2013, enforceable 9/23/2013):

- New regulations affecting the Privacy Rule and Security Rule.
- New regulations implementing HITECH breach and other requirements.
- New regulations implementing GINA (Genetic Information Nondiscrimination Act).
- Extends Security Rules to Business Associates and clarifies both Privacy and Security obligations applicable to subcontractors also.
- New requirements for breach notification, marketing, fundraising, school immunization records, research authorizations and enforcement.

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
To Which Areas Does HIPAA Apply?
Who is covered by HIPAA?

HIPAA applies to:

- **health care providers** who transmit personally identifiable health information 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**, 

Also...

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
Who is covered by HIPAA?

HIPAA applies to:

- Certain health plans:
  - Any individual or group plan, or combination of individual or group plans that provides or pays for the cost of medical care,
  - health insurance issuers,
  - health maintenance organizations, as defined in the Public Health Service Act,
  - issuers of Medicare supplemental policies,
  - long-term care policies (excluding nursing home fixed-indemnity policies),
  - employee welfare benefit plans or other arrangements that are established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers (to the extent that they are not group health plans or health insurance issuers),
  - high risk pools that are mechanisms established under State law to provide health insurance coverage or comparable coverage to eligible individuals,
  - certain public benefit programs, such as Medicare Part A, B and D, Medicaid, the military and veterans’ health care programs, the Indian Health Service program, and others.
A **business associate (BA)** is a person or organization, other than a member of a covered entity’s workforce, that performs certain business functions on behalf of the covered entity and that involves the use, maintenance, or disclosure of protected health information (PHI).

Some of these business functions include: **claims processing, data analysis, utilization review, and billing.** Treatment and research are **not** business associate functions.

Services are limited to: **legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.**

Areas or vendors are **NOT** considered business support components or **associates** if their functions or services do **not** involve the use or disclosure of PHI or where any access would be incidental if at all.

Prior to disclosing PHI to a **business associate**, covered entities are required to enter into a written agreement with the BA that imposes safeguards that the BA will use to protect PHI in its possession. Business associates are now also required to enter into similar agreements with their subcontractors to safeguard PHI received from the BA.
Other entities that the Office for Civil Rights has specifically defined as business associates:

- a Health Information Organization, E-prescribing Gateway,
- Regional Health Information Organization, or other person that provides data transmission services with respect to PHI to a covered entity and that requires routine access to such PHI,
- a person who offers a personal health record to one or more individuals on behalf of a covered entity. When a covered entity hires a vendor to provide and manage a personal health record service the covered entity wishes to offer its patients or enrollees, and provides the vendor with access to PHI in order to do so, the personal health record vendor is a business associate.
Responsibilities of the Covered Entity Relating to HIPAA
What does a covered entity have to do?

A covered entity will:

✖ Name a HIPAA Privacy and Security Officer who will be responsible for compliance with the Privacy, Security Rules and Transactions and Code Set Standards.

✖ Determine and document staff who are covered, their roles and which roles need access to protected health information to do their jobs.

✖ Ensure that all HIPAA policies and procedures are followed and apply sanctions to employees, if necessary, for noncompliance.

✖ Identify business associates of the covered entity and work with the Privacy Officer to ensure that Business Associate Agreements are in place.

✖ Insure that privacy and security safeguards are in place to protect health information in the covered entity’s possession.
What do staff within a covered entity have to do?

- Complete HIPAA training at the frequency specified by the covered entity
- Read the Notice of Privacy Practices applicable to the area in which they work
- Know how HIPAA regulations impact the employee’s individual job procedures
- Sign confidentiality agreements, as necessary.
- Ensure compliance with the “minimum necessary” rule

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
Compliance at Purdue

The Notice of Privacy Practices (NPP) is a document which is distributed to individuals who receive services from the covered entity’s HIPAA-covered health care providers and health plan components.

The document describes how protected health information about individuals may be used and disclosed by the covered entity’s workforce and how the individual can get access to this information.

The NPP for health care providers must be distributed at the first instance of service delivery and posted at the service site and on the website, if one exists. A modified Notice must be posted upon the effective date of the Notice and provided upon request.

The NPP for health plans must be distributed to all new health plan members and at least once every 3 years to current members. Changes to the Notice must be (1) prominently posted on its web site by the effective date of the material change to the notice and (2) provided in a revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan, such as at the beginning of the plan year or during the open enrollment period. The Privacy Rule permits covered entities to distribute their NPPs or notices of material changes by e-mail, provided the individual has agreed to receive an electronic copy.

All covered workforce should read and understand the notice.
Uses and Disclosures of Protected Health Information
The HIPAA Privacy Rule states that PHI should only be used and disclosed:

- for treatment,
- for payment of health care services,
- for healthcare operations,
- as authorized by the patient, and
- For 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.
Using and Disclosing PHI for treatment.

“Treatment” generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

- Clinicians providing treatment services to a patient may share PHI with one another and with providers outside of the covered entity who are known to have a treatment relationship with the patient.

- Staff providing patient instructions or other treatment-related information to a patient or their representative.

- Staff contacting patients to remind of appointments.

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 the information.
Disclosures to Family, Friends and Others Who are Involved in Patient Care or Payment

Staff may disclose protected health information (PHI):

× to any person identified by the individual. The PHI must be directly related to that person’s involvement in the individual’s care or payment for that care.

× to notify a person who is responsible for the care of the individual of the individual’s location or general condition.

You may disclose PHI under these conditions:

If the individual is present or available prior to the disclosure and,

✓ you have asked the individual if it is okay to disclose the information
✓ you have given the individual an opportunity to object, or
✓ you can reasonably infer from the circumstances, based on professional judgment, that the individual does not object

If the individual is not present you may use your professional judgment in determining that it is in the best interest of the individual to:

✓ disclose only the PHI that is directly relevant to a person’s involvement in the individual’s care or payment for care.
✓ allow a person to pick up filled prescriptions, medical supplies, X-rays or other forms of PHI.
Using and Disclosing PHI for Payment

“Payment” encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

- Payment includes such activities as billing insurance companies, patient billing and collection activities, investigating and responding to billing complaints, precertification of services, and obtaining reimbursement from business offices for employee treatment paid for by the department,

- Determining eligibility or coverage under a plan and adjudicating claims;

- Risk adjustments;

- Reviewing health care services for medical necessity, justification of charges, and the like;

- Utilization review activities; and

- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).
Using and Disclosing PHI for Healthcare Operations

Using and Disclosing PHI for healthcare operations.

Healthcare operations are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. Some of the activities include:

- Conducting quality assessment and improvement activities, population based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.
Disclosures of Student Immunizations to Schools

A covered entity is permitted to disclose proof of immunization to a school where State or other law requires the school to have this information prior to admitting the student.

Although, written authorization will no longer be required to permit this disclosure, covered entities will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor.

An agreement to permit the disclosure of immunization records is considered effective until revoked by the parent, guardian or other person acting in loco parentis for the individual, or by the individual himself or herself, if the individual is an adult or emancipated minor. HIPAA additionally requires that covered entities document the agreement obtained under this provision.
HIPAA requires that uses, disclosures, and requests of protected health information (PHI) must be limited to the “the limited data set or if the limited data set is not sufficient, the minimum necessary to accomplish the intended purpose”. This applies to covered components and business associates and their subcontractors.

**Example:** an insurance company requests a patient’s medical record for billing purposes. Only the information pertaining to a specific bill should be sent.

**Minimum necessary does NOT apply to:**

- disclosures of PHI **by a health care provider for treatment purposes,**
- uses or disclosures **made to the individual,**
- uses or disclosures **pursuant to an authorization.**

**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.** Unauthorized access to PHI is prohibited and upon discovery, sanctions may be applied to the employee, up to and including termination, as deemed appropriate given the circumstances.
Compliance at Purdue

**HIPAA Authorizations - Required**

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 **, except for treatment, payment or healthcare operations, uses or disclosures required by law, or for oversight by the originator of the 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.

** Psychotherapy notes are notes stored privately by a psychotherapist regarding therapy sessions. These are NOT part of the medical record.

[http://www.purdue.edu/legalcounsel/hipaa](http://www.purdue.edu/legalcounsel/hipaa)
Phone: 49-66846
legalcounsel@purdue.edu
A HIPAA authorization is **NOT** required when using or disclosing PHI:

- for the purposes of **Treatment**, **Payment** and healthcare **Operations** (**TPO**),
- to the individual or their representative,
- to an entity with whom you have a valid HIPAA business associate agreement,
- as required by law, or in response to a subpoena, discovery request or other lawful process,
- for certain required public health activities,
- for certain activities requested by an employer relating to medical surveillance of the workplace,
- for required disclosures about victims of abuse or neglect,
- for reporting crime, or for purposes of averting a serious threat to health or safety,
- for reviews preparatory to research (by covered entity staff only) and disclosures for research where an IRB waiver has been obtained.
HIPAA protects individually identifiable health information about individuals who have been deceased for up to 50 years after the date of death. After that time, the information is no longer defined as protected health information.

Generally, an authorization is required for a particular use or disclosure of the PHI of a decedent, a covered component may use or disclose the PHI in that situation, only if the covered component obtains an authorization from the decedent’s personal representative, except that certain disclosures are permitted to family members involved in the care of the patient prior to death. (See next slide.)

**Indiana State Law – Personal Representatives**

Indiana State Law dictates who may act as a personal representative for a deceased person.

In the case where a court has appointed a personal representative, one of the following two documents should be presented: a letter of administration (if there is no will) or a letter testamentary (if there is a will).

If there is no court appointed personal representative, then a spouse would be the acting representative. If there is no spouse, any responsible member of the patient's family would be the acting representative, including a parent, guardian, or custodian of the deceased patient's minor child and no documentation would be required in either of these cases, except for appropriate identification.

The representative should sign their own name on the authorization and indicate that they are the decedent’s representative.
Disclosures about a Decedent to Family Members and Others Involved in Care

Covered components are permitted to disclose a decedent’s protected health information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual.

For example, a covered health care provider could describe the circumstances that led to an individual’s passing with the decedent’s sister who is asking about her sibling’s death. In addition, a covered health care provider could disclose billing information to a family member of a decedent who is assisting with wrapping up the decedent’s estate. However, in both of these cases, the provider generally should not share information about past, unrelated medical problems.

Finally, these disclosures are permitted and not required, and thus, a covered component that questions the relationship of the person to the decedent or otherwise believes, based on the circumstances, that disclosure of the decedent’s protected health information would not be appropriate, is not required to make the disclosure.
**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 that covered components obtain an authorization for marketing purposes, except as exempted, and special rules exist where remuneration to the covered component or their business associate is involved.

**Exceptions (no authorization is needed):**

- To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication,

- For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:
  
  (A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual,

  (B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

  (C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.
HIPAA requires authorization for all treatment and health care operations communications where the covered component receives financial remuneration for making the communications from a third party whose product or service is being marketed. The authorization must state that remuneration is involved.

Where a business associate (or the business associate’s subcontractor), as opposed to the covered component itself, receives financial remuneration from a third party in exchange for making a communication about a product or service, such communication also requires prior authorization from the individual.

** If the financial remuneration received by the covered entity is for any purpose other than for making the communication, then this marketing provision does not apply.
A covered component must obtain an authorization for any disclosure of protected health information which is a sale of protected health information. The authorization must state that the disclosure will result in remuneration to the covered entity.

“sale of protected health information” is defined to mean “a disclosure of protected health information by a covered component or business associate, where the covered component or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.” A “sale” is not limited to transactions where there is a transfer of ownership of protected health information.

So, the prohibition on sale of protected health information applies to the receipt of nonfinancial as well as financial benefits.

Also, fees charged to incur a profit from the disclosure of protected health information are not allowed.
**Authorization Requirements - Sale of PHI**

**Exceptions to the Authorization Requirement:**

- **Public Health.** This is whether or not there was any remuneration.
- **Research disclosures** are excepted to the extent that the only remuneration received by the covered component or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for this purpose.
- **Treatment and payment.**
- **Required by law.**
- **Disclosures to the individual** to provide access to PHI or an accounting of disclosures, where the fees charged for doing so are in accord with the Privacy Rule.
- **Remuneration paid by a covered component to a business associate** for activities performed on behalf of the covered component, as well as remuneration paid to a covered component to cover the cost to prepare and transmit the PHI for any disclosure otherwise permitted by the Privacy Rule.
- **Uses of PHI within a covered entity,** as the prohibition applies only to disclosures outside of a covered entity.
- **Disclosures of limited data sets for purposes permitted under the Rule** would be exempt from the authorization requirements to the extent the only remuneration received in exchange for the data is a reasonable, cost-based fee to prepare and transmit the data or a fee otherwise expressly permitted by other law.
- Can charge for reasonable **costs of reproducing records given to a patient** so long as costs are actual costs and do not generate any profit.
**Fundraising Requirements**

**Definition:** A communication to an individual that is made by a covered component, an institutionally related foundation, or a business associate on behalf of the covered component for the purpose of raising funds for the covered component is a fundraising communication. The notice and opt out requirements for fundraising communications apply only where the covered component is using or disclosing protected health information to target the fundraising communication.

**Notice of Privacy Practices**

The notice of privacy practices must inform individuals that a covered component may contact them to raise funds for the covered component and an individual has a right to opt out of receiving these communications.

**Opt Out:**

A covered component must provide, with each fundraising communication sent to an individual, a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications.

Covered components are also free to provide individuals with the choice of opting out of all future fundraising communications or just campaign specific communications. Whatever method is employed, the communication should clearly inform individuals of their options and any consequences of electing to opt out of further fundraising communications. The final rule does not require covered components to send pre-solicitation opt outs to individuals prior to the first fundraising communication.

**Opt In:**

The opt out will remain in affect until the individual opts back in. The method of opting in is up to the discretion of the covered component, but the individual must take action to opt in. Automatic opt in’s or opt out expirations are not allowed.
HIPAA prohibits covered health plans from using or disclosing PHI that contains genetic information for underwriting purposes, except for issuers of long term care policies. This prohibition applies to all genetic information from the compliance date (9/23/2013) going forward, regardless of when or where the genetic information originated.

“genetic information” is defined to mean, with respect to any individual, information about:

1. an individual’s genetic tests;
2. the genetic tests of family members of the individual; and
3. the manifestation of a disease or disorder in family members of the individual (i.e., family medical history). The term “genetic information” also includes, with respect to any individual, any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by an individual or family member of the individual.

“underwriting purposes” does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

Also, health plans covered by those rules are restricted from requesting genetic information.

To the extent that an individual’s genetic information is needed for the treatment purposes of a family member, a covered health care provider is permitted to disclose this information, subject to any agreed-upon restriction, to another provider for the treatment of the family member.
An inadvertent disclosure is a disclosure of PHI made by staff in a covered component which violates the Privacy Rule. This would include impermissible uses or disclosures or disclosures that violate the minimum necessary provision.

These inadvertent disclosures need to be reported to your supervisor.

- Your supervisor will ensure that the disclosure is tracked as required and will send a copy to the HIPAA Privacy Officer for identification of any requirements to report to the individual and Health and Human Services (e.g. breach reporting).

Examples of inadvertent disclosures include:

- a label listing patient1’s identifying information was placed on patient2’s discharge document and given to patient2.

- A conversation between 2 staff members of the health plan about an individual’s claim issue occurred in an elevator and was overheard by another person who did not have a legitimate reason to know.

- A document containing protected health information was faxed to the wrong fax number.

- More than the minimum necessary information was provided to an insurance carrier during the billing process.
Compliance at Purdue

Breach Reporting

When a disclosure of PHI occurs that violates the Privacy Rule, there is an assumption that a breach occurred. HIPAA allows the covered entity to conduct a risk assessment to determine whether the disclosure is a breach that is reportable to the individuals affected, to the Office for Civil Rights or to the covered entity who provided PHI to a business associate.

There are three ways in which a breach may be identified:

- an inadvertent disclosure of PHI by workforce of the covered entity,
- a breach of unencrypted electronic data maintained by the covered entity that includes PHI,
- any unauthorized use or disclosure by workforce of one of the covered entity’s business associates or its agents or subcontractors.

In all cases, the disclosure will be reported to the HIPAA Privacy Officer who will determine whether the disclosure is a breach and, if so, will take the necessary steps to address the HIPAA reporting requirements.

Should a reportable breach occur, the covered entity must make notification without unreasonable delay and within 60 days of discovery of the breach, unless a law enforcement delay has been requested. Reporting to the HIPAA Privacy Officer, therefore, needs to occur as soon as a potential breach is discovered.

A breach is defined as the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy rule, which compromises the security or privacy of the protected health information.
Rights Of The Individual
Individual’s Access to PHI

Individuals have the right to inspect, access, or obtain copies of their own protected health information, except:

- psychotherapy notes,
- information compiled for use in a civil, criminal or administrative action or proceeding,
- PHI that is exempt from the Clinical Laboratory Improvements Act or as prohibited by law,
- in certain situations where treatment was provided as part of a research study and the individual agreed to the denial of access, when consenting to participate, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research,
- if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

These are grounds for denial for which an individual does not have the right to request a review.

When PHI is released to the individual by a healthcare provider, a written authorization must be obtained to document the disclosure in accordance with state law.

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
Compliance at Purdue

**Individual’s Access to PHI**

**Reviewable grounds for denial.** A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed,

- A licensed health care professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- The PHI makes reference to another person (unless the other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to this other person; or
- The request for access is made by the individual’s personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm 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 reviewing official and who did not participate in the original decision to deny.

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
Requests for Electronic PHI

If an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic format requested by the individual, if it is readily producible, or, if not, in a readable electronic format as agreed to by the covered entity and the individual. Covered entities must provide individuals with some kind of readable electronic copy and images, must be included, if requested.

For example, this would include providing the individual with an electronic copy of the PHI in the format of MS Word or Excel, text, HTML, or text based PDF, among other formats.
Individual’s Access to PHI

Timeliness
The covered entity must act on a request for access no later than 30 days after receipt of the request. A covered entity can have a one-time extension of 30 days to respond (with written notice to the individual of the reasons for delay and the expected date by which the entity will complete action on the request).

Costs
Any fee imposed by the covered entity for providing an electronic copy shall not be greater than the entity’s labor costs in responding to the request for the copy plus the cost of supplies for creating the paper copy or electronic media (i.e., physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. A covered entity is permitted to charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier.

Third Parties
If requested by an individual, in writing, a covered entity must transmit the copy of PHI directly to another person designated by the individual.

Request
Although HIPAA does not require an authorization for release of medical records to the individual or their representative, when this type of release occurs, a written request for the record must be obtained to document the disclosure, in accordance with Indiana state law. Generally, the HIPAA authorization is used for this purpose.
Amendment Requests

A covered entity is required to act on the individual’s request for an amendment of their PHI no later than 60 days after receipt of the request.

An extension of one 30-day period is allowed, provided that within the initial 60-day period, the individual is notified in writing of the reason for the delay and the date by which action on the amendment will be completed.

The covered entity is not required to agree to the amendment if the protected health information or record that is the subject of the request:

- Was not created by the covered entity and the individual has not provided a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment.
- Is confidential and not available for inspection.
- Is not part of the set of records designated as covered by HIPAA.
- Is accurate and complete.

The covered entity must also identify other entities which were provided the un-amended information and may rely upon it in the future, and then send the amendment to them. Therefore, all requests for amendment will be reviewed by the HIPAA Privacy Officer.
Disclosure Tracking—Required

HIPAA regulations grant individuals the right to receive an accounting of certain “trackable” disclosures of their PHI made by a covered entity for the six years prior to the request.

In order to meet this requirement, the following disclosures must be tracked by the covered entity and maintained in either the medical record (if applicable) or by the covered entity’s HIPAA Privacy Officer:

- **Required by law** (i.e. reports of abuse to a public health authority)
- **Required for public health activities** (i.e. reporting of disease to the Indiana State Department of Health)
- **Reports of abuse** (i.e. Child Protective Services)
- **For health oversight activities** (i.e. audits by an oversight agency)
- **For judicial and administrative proceedings** (i.e., Subpoenas, court orders, etc.)
- **For law enforcement purposes** (i.e. to identify the perpetrator of a crime)
- **For research** (i.e. Where the researcher has obtained a waiver, but not where an authorization was obtained or pursuant to a limited Data Set Agreement)
- **To the coroner** (i.e. for identifying a deceased person)
- **To avert a threat of serious injury** (i.e. disclosure to a person who can prevent the threat or to law enforcement)
- **Unlawful or unauthorized disclosures** (i.e. inadvertent disclosures)

**Note:** Inadvertent disclosure forms must be completed and provided to the HIPAA Privacy Officer who will determine whether breach notification is required.
Disclosure Tracking Documentation

Certain information is required to be tracked, therefore, a Record of Disclosure form is used to record the required information. If some other method is used to record these disclosures, for example, an entry made in the medical record, it is not necessary to also record the information on that Record of Disclosure form.

Inadvertent disclosures, accidental disclosures of PHI, are tracked using the Inadvertent Disclosure form. This form is filled out by the person who made or discovered the inadvertent disclosure and provided to the HIPAA Privacy Officer for investigation.

The following information is required to be collected:

- date of disclosure,
- name of the entity or person receiving the information,
- brief description of PHI disclosed, and
- brief purpose of the disclosure.
Disclosures of PHI that do NOT need to be tracked include, those:

- for Treatment, Payment, Healthcare Operations,
- to the patient or their representative,
- where an authorization has been obtained,
- uses and disclosures to those who are involved in the individual’s care where authorized by the patient,
- disclosures to a covered component’s business associate in accordance with the Business Associate Agreement,
- for national security or intelligence.
The covered entity’s health care providers will **accept and accommodate reasonable requests by individuals to receive PHI through alternative means or at alternative locations.**

**Health Care Providers** **may not require an explanation from the individual as to the basis for the request** as a condition of providing communications on a confidential basis.

**Covered health plan(s)** will accept verbal requests for confidential communications on a single-event basis. The health plans **may require that all requests for confidential communications include a statement from the individual that disclosure of all or part of the information, to which the request pertains, could endanger the individual.**

**Examples** of these kinds of requests are:
a request to send bills for treatment to an on-campus address, to return a phone call to a specific phone number or to speak to a health plan member in a private office.
Restrictions

- Individuals have the right to request a restriction of the use and disclosure of their PHI for the purposes of treatment, payment or healthcare operations or for involvement in the individual’s care and notification purposes. The request must be promptly reviewed.

  The covered entity is generally, not required to agree to these types of restrictions, but if approved, all covered components must abide by the restriction, except in emergency circumstances when the information is required for the treatment of the individual.

- If the request for restriction is on disclosures of PHI to a health plan or their business associate, for the purpose of carrying out payment or health care operations and if the restriction applies to PHI that pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full, the covered entity must comply with the restriction, if the disclosure is not otherwise required by law (e.g. Medicaid).

- If payment is dishonored, the health plan may be billed but only after the provider has made a reasonable effort to contact the individual and obtain payment.

- For all other requests for restricted disclosure of PHI, notify your supervisor.

- In the case where a patient wishes to restrict disclosures to the health plan by a downstream provider, e.g. pharmacist, the patient should be counseled to make the request directly to the Pharmacy or other covered component. A paper prescription may be provided to eliminate the automatic disclosure to insurance prior to the patient’s arrival at the Pharmacy.

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
Complaints

Individuals have the right to file a complaint with the Covered Entity’s Privacy Officer or with Health and Human Services. Should you be approached with a privacy complaint, notify your supervisor immediately.

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
General Safeguards – Spoken PHI

Protecting spoken protected health information includes:

✖ Business Support Components should direct questions from individuals about bills or other PHI to the originating provider or health plan staff who can answer detailed questions,

✖ Confidential verbal conversations should be conducted away from others who do not need to know. Close doors or conduct discussions about PHI with individuals in a private office. Do not use patient names in public areas like waiting areas, hallways or elevators,

✖ Ask the individual’s permission before speaking about their PHI in front of others accompanying them,

✖ Speak softly when discussing PHI in areas where discussions could be overheard,

✖ Never use or disclose confidential information for any personal purpose or out of curiosity, or allow others to do so.
General Safeguards – Paper PHI

To safeguard protected health information on paper, you must:

☒ Never leave papers unattended on printers, copiers, fax machines, etc.,

☒ Use a cover sheet when faxing PHI and check the fax number prior to using if unsure of the number,

☒ Documents containing PHI should not be left in open areas or on desks where they can easily be seen by passers by. Place these documents in folders, turn them over or place a sheet of paper on top,

☒ Shred papers containing PHI when no longer needed or place in approved confidential destruction bins. Don’t throw it in the trash!

☒ If “lost” papers are found, give to the HIPAA liaison in the area,

☒ Ensure that appropriate physical safeguards are used to safeguard papers when not in use, like placing in locked file cabinets.

☒ Rooms and file cabinets where PHI is stored should be locked whenever staff are out of the office.
Safeguarding **electronic PHI** means you should:

- Computer screens where PHI is viewed should be either turned away from the view of visitors or applications should be minimized while not in use.

- Do not ever disclose your user id or password to anyone (even computer support staff), or allow anyone to access or alter information under your identity. Passwords should NEVER be posted near the work area or in a place that is easily accessible by other people.

- A password-protected screen saver or application timeout is required on all workstations in HIPAA-covered areas. Always lock your workstation when leaving your work area for more than a few minutes.

- **NEVER** copy files containing PHI to an unencrypted laptop or mobile device (i.e. palm Blackberry or FLASH drives). The covered entity may have specific rules about using laptops or mobile devices. If they have not been communicated to you, ask your supervisor prior to using them.

- Strong passwords for systems storing PHI should be used in all cases, where possible.

---

[http://www.purdue.edu/legalcounsel/hipaa](http://www.purdue.edu/legalcounsel/hipaa)
Phone: 49-66846
legalcounsel@purdue.edu
General Safeguards

- Obligations to safeguard private information continue after you leave employment at Purdue or a move to a different position at Purdue.
- Notify your supervisor if someone you don’t know is in the building or doing something that appears suspicious.
- All fraudulent attempts to obtain PHI should be reported to the supervisor, who will report according to the Incident Response Policy.
- Information containing PHI should not be removed from the facility unless necessary for limited purposes, such as transfer to a storage facility or to a physician for treatment purposes and approved by your supervisor. Paper documents should be stored in a locked trunk of a car and immediately removed upon arrival at the destination. If information must be kept in the car, store it where not visible and in lockable attaches, lock boxes, or other secure opaque containers. Electronically stored documents must be encrypted when stored or transmitted using an approved encryption method. Documents containing PHI should **NEVER** be removed from the facility for “work at home” purposes.

**Note:** _Never change the configuration of your Purdue workstation without prior approval of your workstation support group._

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu
If you have any questions about HIPAA and when or what protected health information you can use or disclose, **ask your supervisor.**

If your supervisor is unavailable, **call the covered entity’s HIPAA Privacy Officer.**

http://www.purdue.edu/legalcounsel/hipaa
Phone: 49-66846
legalcounsel@purdue.edu