Health Insurance Portability and Accountability Act of 1996
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Federal law passed by Congress
- 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.
- Creates a framework, using standardized formats, for transmitting electronic health information more cost effectively.

Generally, all employees working in a covered entity are covered by the HIPAA regulations and must comply with its requirements. Purdue is a hybrid entity which means only those areas who meet the coverage criteria are covered.
What is Protected Health Information (PHI)?

The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

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

**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 the individual or can be used to identify the individual.

**PHI includes many common identifiers** (for example: name, address, birth date, medical record number).
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 owns 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 the covered entity’s Human Resources department.

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

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
Penalties for Noncompliance-Civil

HIPAA's enforcement provisions authorize the Secretary to impose penalties to non-complying entities.

**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 circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.

*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.
The HIPAA regulations are comprised of three parts:

- The Privacy Rule
- Transactions and Code Set Standards
- The Security Rule

Note: Changes that are part of the HITECH Act, effective 2/17/10, are incorporated where applicable in the training.
The Privacy Rule:

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

- **identifies permitted uses and disclosures** and,

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

- **requires sanctions to be applied** to employees who violate HIPAA policies and procedures.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
### Transactions and Code Set Standards

#### The Transactions and Code Set Standards:

- Electronic data interchange (EDI) is the electronic transfer of information between trading partners, for example, medical health claims transmitted electronically between a healthcare provider and insurance company.

- The Transaction and Code Set Standards establish required formats and standardized content for a defined set of transactions. Also, specific code sets (i.e. diagnostic codes) are required to be used in those transactions.

- The purpose of this standardization is to **increase the efficiency of EDI** and **decrease costs to healthcare providers and health plans**.
### The HIPAA Security Rule:

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

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

- **Excessive**
  - 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.

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

---

**Compliance at Purdue**

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
To Which Areas Does HIPAA Apply?
Who is covered by HIPAA?

HIPAA applies to:

- individual or group health plans, or a combination thereof, that provides, or pays for the cost of medical care,
- health care clearinghouses,
- health care providers who transmit personally identifiable health information in electronic form in connection with one of the transactions defined within the Transaction and Code Set Standards under HIPAA.

Also…

Compliance at Purdue

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
Who is covered by HIPAA?

HIPAA also applies to:

- Vendors that have access to protected health information and that provide certain business functions or services on behalf of covered healthcare providers or covered health plans.

Some of these functions include:

  claims processing, data analysis, utilization review, and billing.

Services are limited to:

  legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

- These areas within the covered entity are covered as business support components. Vendors outside of the covered entity are referred to as business associates.

- 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.
HIPAA Business Associates

A **business associate (BA)** is a person or organization, other than a member of the covered entity’s workforce, that performs business functions on behalf of the covered entity that involve the use or disclosure of protected health information (PHI).

**Business Associates** are covered entities under HIPAA and are directly accountable for compliance with the regulations.

Prior to disclosing PHI to a **business associate**, the covered entity is required to enter into a written agreement with the BA that imposes safeguards that the BA will use to protect the PHI while in its possession.
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.
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.

The NPP for health plans must be distributed to all new health plan members and at least once every 3 years to current members.

- All covered employees should read and understand the notice.
Uses and Disclosures of Protected Health Information

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
Using and Disclosing PHI

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,
- For other circumstances described in the Privacy Rule.

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

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 Purdue 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.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
Using and Disclosing PHI for Healthcare Operations-Communications

In general, a communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall be considered a healthcare operation (not requiring an authorization), if the communication is 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,
- for treatment of the individual, or
- is for case management or care coordination or
- to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Not considered healthcare operations and what would require an authorization prior to the communication:

- if the covered entity receives or has received direct or indirect payment in exchange for making the communication, except
  - where the communication describes only a drug or biologic that is currently being prescribed for the recipient, and any payment received by the CE in exchange for making the communication is reasonable in amount,
  - the communication is made by the covered entity and the covered entity obtains from the recipient, a valid authorization, or
  - the communication is made by a business associate on behalf of the covered component and the communication is consistent with the written business associate agreement.
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”

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.
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,
- any other use or disclosure inside or outside of the covered entity 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.

- The covered entity’s HIPAA authorization form should be used when an authorization is obtained from a patient or if on another entity’s form, reviewed by the Privacy Officer for validity.
**HIPAA Authorizations - NOT Required**

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.
Inadvertent Disclosures

An **inadvertent disclosure** is a disclosure of PHI made by staff in a covered entity which should not have occurred.

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 (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.
When a breach of PHI occurs, an assessment is required to determine whether the breach is reportable to the individual and to the Secretary of Health and Human Services, as is required by HIPAA in certain circumstances.

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

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

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

Should a reportable breach occur, the covered entity must make notification within 60 days of discovery of the breach, therefore, reporting to the HIPAA Privacy Officer needs to occur as soon as a potential breach is discovered.

A breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which poses a significant risk of financial, reputational, or other harm to the individual, excluding any stated exceptions.
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.

In the case that a covered entity uses or maintains an electronic medical record, the individual has the right to obtain a copy of their PHI in an electronic format and, if desired, to direct the to transmit the copy directly to an entity or person designated by the individual, covered entity provided that the request is clear and specific. Any fee the covered entity may charge, cannot be greater than the entity’s labor costs in responding to the request.

- 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.

These are grounds for denial for which an individual does not have the right to request a review.
Individual’s Access to PHI

Reviewable grounds for denial

A covered entity may deny an individual access to their PHI, in the following circumstances:

✖️ 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 such 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, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny.
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.**
Disclosure Tracking - NOT Required

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,
- for national security or intelligence.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
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:

- 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

IMPORTANT:

✗ If the individual requests communication via e-mail, they should be advised that e-mail is not a secure method of communication and that the covered entity is prohibited from communicating PHI using e-mail.
Restrict the use or disclosure of their PHI:

- Individuals have the right to request a restriction of the use and disclosure of their protected health information 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 not required to agree to these types of restrictions, but if approved, the entire covered entity must abide by the restriction.

- Individuals also have the right to request that a covered entity not disclose PHI to a health plan when, the disclosure is not otherwise required by law and the disclosure is for purposes of payment or healthcare operations and the PHI pertains solely to a health care item or service that the provider involved has been paid out of pocket in full.

In this case, the covered entity must comply with the restriction.

- All requests for restricted use of PHI for the purposes of treatment, payment or healthcare operations will be reviewed by the HIPAA Privacy Officer.
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.
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 discuss PHI 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.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
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.
General Safeguards – Electronic PHI

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 a laptop or mobile device (i.e. palm Blackberry or FLASH drives). PHI should NEVER be stored on a C: drive if a network drive is available for storage.

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

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
General Safeguards

- Obligations to safeguard private information continue after you leave employment by the covered entity or a move to a different position in the covered entity.
- 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 entity’s Incident Response Policy.

Note: Never change the configuration of your workstation without prior approval of your workstation support group.
HIPAA and Research
HIPAA protections extend to research, establishing the conditions under which covered entities might release personally identifiable health information for research purposes.

Human Subject Research requires

☐ approval by the IRB prior to the commencement of the project.

http://www.purdue.edu/hipaa
Phone:  49-61927
hipaa-privacy@purdue.edu
The basic rule is that research is not part of “treatment”, “payment” or “healthcare operations”, therefore the researcher must obtain a HIPAA authorization prior to receiving any protected health information for use in research.

Exceptions to this rule:

- IRB waiver
- IRB modifications of authorization requirements
- Reviews preparatory to research by staff of the covered entity
- Research involving a decedent’s information
- Use of a limited data set
**De-Identified Information**

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.
IRB Waiver or Modification

A researcher can seek a **waiver** of the authorization requirement or a **modification to the requirements** from the IRB.

In order to obtain the waiver, the researcher must satisfy the IRB regarding the following criteria:

1. 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.

2. The research could not practicably be conducted without the waiver or alteration to the authorization; and

3. The research could not practicably be conducted without access to and use of the PHI
Approval of Waiver or Modification
Covered Entity Requirements

- If the criteria are met, the IRB must provide and maintain documentation of the waiver.
- The covered entity may **NOT** disclose the PHI without receiving **ALL** of the following:
  1. **Identification of the IRB** and the date on which the alteration or waiver of authorization was approved;
  2. **A statement** that the IRB has determined that the alteration or waiver of authorization, in whole or in part, **satisfies the required criteria**;
  3. **A brief description of the PHI** for which use or access has been determined to be necessary by the IRB;
  4. **A statement** that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
  5. **The signature of the chair or other member**, as designated by the chair of the IRB, as applicable.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
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.

A staff member of the covered entity can recruit participants on behalf of the researcher. Once contacted, a patient could then choose to participate and could sign an authorization giving the researcher access to their PHI.
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:

1. the use or disclosure of the PHI is solely for research on the PHI of a decedent,
2. that the PHI sought is necessary for the research, and
3. at the request of the covered entity, that documentation of the death of the affected Individuals be provided.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
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.
Compliance at Purdue

Minimum Necessary - Research

- If the authorization requirement is waived by the IRB, requests, uses and disclosures of protected health information 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"

- Also, access to and use of the information should be limited to only those researchers or others who need access to protected health information to carry out their duties, and

- All protected health information must be maintained in a secure environment to ensure limited access to protected health information and to avoid incidental disclosures of protected health information.

http://www.purdue.edu/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu
The Privacy Rule requires covered entities to account for certain disclosures made after April 14, 2003, for a period of six (6) years, if requested to do so by an affected individual.

A covered entity must account for disclosures made pursuant to an IRB waiver.

The response must include:
- the name of the researcher,
- his/her contact information,
- the name of the study,
- a description of the purpose of the study,
- the type of protected health information sought, and
- the time frame of disclosures in response to the request.

The covered entity must also assist the individual in contacting those researchers to whom disclosure was likely made, if requested to do so.
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/hipaa
Phone: 49-61927
hipaa-privacy@purdue.edu