Health Insurance Portability and Accountability Act of 1996

Research Version

http://www.purdue.edu/hipaa
hipaa-privacy@purdue.edu

As of 3/14/2016
PII or **personally identifiable information** is any data that can be used to contact, locate or identify a specific individual, either by itself or combined with other sources that are easily accessed. It can include information that is linked to an individual through financial, medical, educational or employment records.

Examples of data elements that can identify an individual include name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number.

Under certain circumstances, one or two pieces of data can be brought together with other easily-accessible information to create a vulnerability for someone’s identity. Even if the pieces of data seem to be harmless when by themselves.

Safeguarding PII and other sensitive information is the responsibility of federal agencies.

Examples of laws related to different types of PII are listed below:

- HIPAA/HITECH - Health related information
- GLBA - Financial information
- Privacy Act - Fair Information Practices for PII held by Federal Agencies
- COPPA - Protects children’s privacy by allowing parents to control what information is collected
- FERPA - Student’s personal information
- FCRA - Collection and use of consumer information

Such laws attempt to restrict corporations from inappropriately sharing PII and impose requirements for appropriately protecting such information.
What is HIPAA?

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 components.

✗ Creates a framework, using standardized formats, for transmitting electronic health information more cost effectively.

*** All departments and workforce designated by Purdue’s HIPAA Privacy Officer as HIPAA covered components, must comply with its requirements.
The HIPAA legal requirements have evolved over several years, and include:

- HITECH (2010)
- 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.
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.
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** 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.

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.
Some examples of protected health information at Purdue include:

- **Treatment or other patient information** maintained by Purdue’s medical, mental health and dental clinics,
- **Prescription information** processed by the Purdue Pharmacy,
- **Health claims** processed by Purdue’s health plan administrators,
- **Clinic billing information**, processed by the Accounts Receivable department,
- **Treatment or accounts receivable information** accessed by ITaP while providing support to Purdue’s covered components,
- **Protected health information** used by Purdue researchers.
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 Purdue 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

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 Office for Civil Rights has provided guidance regarding methods of de-identification for protected health information:

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.
The HITECH Act (2010) requires Health and Human Services to develop procedures by which an individual harmed by a HIPAA breach of health information may obtain a percentage of the HHS enforcement penalty.

This process was expected to be announced sometime in 2015.
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 to obtain damages, or to forbid further violations of the HIPAA Privacy and Security Rules.

Health and Human Services 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.
Attorneys

Civil Lawsuits

There is no private right of action under HIPAA, however, attorneys in Indiana and in several other states are now using HIPAA as a “standard of care” and are suing on behalf of individuals for HIPAA violations.
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)
- **health care clearinghouses.**

Also…

http://www.purdue.edu/hipaa
hipaa-privacy@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.

Also…
A business associate (BA) is a person or organization, other than a member of a covered entity’s workforce, that performs payment or healthcare operations 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.

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.

Purdue covered provider

or health plan → Purdue PHI → Vendor

(e.g. PUSH → software vendor)
HIPAA Business Associates

✖ Business Associates and their Subcontractors

A Business Associate’s subcontractors and agents are also required to comply with many of the HIPAA regulations and other requirements.

Purdue covered provider
   or health plan → Purdue PHI → Vendor → vendor subcontractor
   (e.g. PUSH → software vendor → vendor’s consultant)
Purdue’s covered components can also be Business Associates. Some departments at Purdue provide business functions on behalf of covered entities outside of Purdue.

These departments are referred to as **Internal Business Associates** and use PHI to provide services for these outside entities. Examples of these services are data aggregation and work flow analysis.

Outside Covered Entity → Covered Entity PHI → Purdue
(e.g. hospital → Regenstrief)
Departments within Purdue who perform business functions that require access to or use of PHI for Purdue’s covered healthcare providers or health plans are referred to as **Business Support Components**. They are covered by HIPAA and must comply with the regulations.

Purdue covered provider
  or health plan  →  Purdue PHI  →  Purdue covered department
(e.g. PUSH  →  Accounts Receivable)
Business Associate Agreements

Covered entities who share PHI with business associates are required to execute a Business Associate Agreement (BAA) prior to disclosing the PHI.

These written agreements impose safeguards that the BA will use to protect PHI in its possession, for example,
- allowable uses and disclosures,
- reporting of breaches to the covered entity, and
- general compliance with the HIPAA Privacy and Security Rules.

Business associates who share PHI with subcontractors or agents must also execute Business Associate Agreements with these entities. The entity must adhere to the same restrictions and conditions on the use or disclosure of PHI that apply to the business associate.
The OCR guidance states specifically that researchers are not business associates:

Other Situations in Which a Business Associate Contract Is NOT Required

“To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of “business associate” at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.”

- There can be some projects, however, involving a research component and a healthcare operations component. For example, testing the application of research results. The healthcare operations component of a project would require us to sign a BAA in order to access identifiable data in reviewing processes at a facility.

- Also, if a researcher contracts with an outside entity to store or aggregate PHI on their behalf, we would need to ensure that a Business Associate Agreement is in place to protect the data.
**How does HIPAA impact Purdue?**

- Purdue University has been designated as a **hybrid entity** under the HIPAA Privacy Regulations.

- Purdue’s primary purpose is education; however, Purdue has departments that meet the criteria for HIPAA coverage.

- All of Purdue University is **NOT** covered by HIPAA, only those areas that have been formally designated as covered components by the HIPAA Privacy Officer. However, Purdue is ultimately responsible for compliance by its covered components.

A list of departments at Purdue that are covered by HIPAA can be found at: [http://www.purdue.edu/push/HIPAA/CoveredComponents/index.html](http://www.purdue.edu/push/HIPAA/CoveredComponents/index.html)
The following areas have been designated as **COVERED COMPONENTS** at **Purdue**:

### Healthcare Providers:
- Purdue Student Health Center
- Purdue Pharmacy
- Purdue’s North Central Nursing Clinics
- Nursing Center for Family Health
- Purdue’s SLHS Audiology and Speech-Language Clinics
- Lafayette Street Family Health Clinic
- IPFW Dental Hygiene Clinic
- IPFW Center for Healthy Living:
  - Campus Clinic and Wellness Programs
- Purdue Sports Medicine WL

### Health Plan:
- Purdue Self-Insured Medical Benefits Plan(s)
- Vision Plan
- Pharmacy Plan(s)
- Health Care Flexible Spending Account Plan
- Health Care Retirement Accounts
- Employee Wellness Programs

[http://www.purdue.edu/hipaa](http://www.purdue.edu/hipaa)

hipaa-privacy@purdue.edu
## Who is covered at Purdue?

### Business Support:

<table>
<thead>
<tr>
<th>Student and Receivables Business Services-Accounts Receivable</th>
<th>North Central Information Services</th>
<th>RCHE-Health Outcomes and Policy Research Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITaP (only Operating Systems Platform, Basis Administration, Database Administration, Production Control, Student System Administration, Telecommunications, Data Center &amp; Enterprise Storage, Application Services, Security Services, Identity and Access Management Office, Service Desk and Desktop Computing Services, IT Research Computing, Project Management Office)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Records</td>
<td>SLHS Business and Main Offices</td>
<td>SLHS Electronics and Technical Support</td>
</tr>
<tr>
<td>School of Nursing Business Office</td>
<td></td>
<td>Risk Management</td>
</tr>
<tr>
<td>Bursar</td>
<td></td>
<td>Central Files</td>
</tr>
<tr>
<td>Environmental Health</td>
<td></td>
<td>Pharmacy IT</td>
</tr>
<tr>
<td>Student and Receivables Business Services-Loans</td>
<td></td>
<td>Purdue Student Health Center</td>
</tr>
<tr>
<td>IPFW School of Health Sciences Business Office</td>
<td></td>
<td>Calumet Technological Infrastructure Services</td>
</tr>
<tr>
<td>IPFW Information Technology Services</td>
<td></td>
<td>Calumet Procurement &amp; General Services</td>
</tr>
<tr>
<td>Athletics Information Systems</td>
<td></td>
<td>Health and Human Sciences IT</td>
</tr>
<tr>
<td>Regenstrief Center for Healthcare Engineering</td>
<td></td>
<td>Calumet Fitness Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Center for Medication Safety Advancement</td>
</tr>
</tbody>
</table>

(continued…)
Who is covered at Purdue?

Business Support (continued):
- Technology Statewide Business Offices
- Digital Education
- Healthcare Advisors
- IPFW Accounts Payable
- North Central Purchasing
- North Central Bursar
- Comptroller
- Purdue Recycling
- Payment Processing
- Treasure Operations
- Legal Counsel for Purdue University

Purdue Internal Business Associates
- Healthcare Advisors
- Regenstrief Center for Healthcare Engineering
- Center for Medication Safety Advancement
- IT Research Computing
- HHS Minnesota DHS Evaluation Projects
- Center for Cancer Research
- Cost Effectiveness of Novel Nasal Nebulizer-Delivered Budesonide as an Alternate to Surgery for the Treatment of Nasal Polyps Project
In most cases, research requesting PHI from Purdue’s covered components will include Purdue’s covered providers, health plans or internal business associates.

Business support components do not own the data and will refer researchers to the data owners to request PHI.
HIPAA and Research
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 at Purdue requires
  - approval by the Purdue IRB prior to the commencement of the project.

- The *Human Research Protection Program* may be contacted for Purdue research-related questions at (765) 49-45942 or irb-questions@purdue.edu

- *Joan Vaughan*, may be contacted for any HIPAA-related question at x61927 or jvaughan@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. (Form: Authorization for Release or Use of Protected Health Information for Research Purposes)

Exceptions to this rule:

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

(Please refer to the Purdue University Research Guidelines for Compliance with HIPAA Privacy Rule)
Compliance at Purdue

http://www.purdue.edu/hipaa
hipaa-privacy@purdue.edu

**IRB Waiver or Modification**

A Purdue researcher can seek a *waiver* of the authorization requirement or a *modification to the requirements* from Purdue’s IRB. *(Form: Application for Waiver of Authorization Modification of Authorization Under HIPAA Privacy Rule)*

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 Component Requirements

- If the criteria are met, the IRB must provide and maintain documentation of the waiver (*Form: Approval of Request for Waiver, Partial Waiver or Modification of Individual Authorization for Disclosure of Protected Health Information*)

- The covered component 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.
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.

Minimum necessary is a reasonableness standard that requires covered entities to make their own assessment of what PHI is reasonable necessary for a particular 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 to or requests by a health care provider for treatment purposes,
- uses or disclosures made to the individual,
- uses or disclosures pursuant to an authorization,
- uses or disclosures to Health and Human Services, or
- uses or disclosures that are required by law or required for compliance with the HIPAA privacy rule.
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”

- Even when an authorization is required, researchers must consider and request access to only the data necessary to achieve the goals of the research project.

- 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.

Secure storage and transmission is required for identifiable PHI and limited data sets. The researcher’s IT support area is responsible for implementation of the safeguards. ITaP Security and Policy can be consulted for assistance. Karen Monkhouse will provide guidance on the minimum requirements to safeguard the information.
Reviews Preparatory to Research

When a researcher is part of the workforce of a covered component, the covered component 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.

(Form: Certification of Compliance with HIPAA Privacy Rule Regarding Activities Preparatory to Research)

A researcher who is not part of the covered component’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 component 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 component 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 component, that documentation of the death of the affected Individuals be provided.

(Form: Certification of Compliance with HIPAA Privacy Rule for Research Involving Decedent’s Information Only)

The covered component will be responsible for obtaining the certification of compliance and any necessary death certificates.
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 component, 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 Purdue IRB. **(Form: Data Use Agreement)**
**Data Use Agreements**

A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of the information by the recipient. The data use agreement may not authorize the recipient to use or further disclose the information in a manner that would violate HIPAA, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the recipient will:

1. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
3. Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
4. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
5. Not identify the information or contact the individuals.

- Other types of "Data Use Agreements" are sometimes provided to define the safeguards required by a recipient of data but that are not Data Use Agreements for use with a Limited Data Set as described above.

- I prefer to name these other types of agreements "Use of Data Agreements" to avoid confusion about use of PHI.
Data Use Agreements

- If a limited data set is disclosed by a Purdue covered component to a Purdue researcher, the Data Use Agreement will be signed by the covered component and the PI.

- Where the limited data set is disclosed by an outside covered entity to a Purdue researcher, the Data Use Agreement will be signed by the covered entity, the PI and also Sponsored Program Services.
Covered components and researchers have flexibility to describe the information to be used or disclosed for future research, so long as it is reasonable from the description to believe that the individual would expect the information to be used or disclosed for future research. A description of the PHI to be used for the future research may include information collected beyond the time of the original study.

A researcher may request authorization to use information obtain for future research purposes, as long as the authorization includes sufficient clarity such that a reasonable individual would expect his or her PHI will be used or disclosed for future research.
Uses and disclosures pursuant to an authorization are permissive and not required, and thus, a covered component may cease using or disclosing PHI pursuant to an authorization based on an individual’s oral request if it chooses to do so.

Written revocations must however, be accepted and uses or disclosures under the authorization must cease, except to the extent the covered component has relied upon it and except to maintain the integrity of the research.
Accounting for Research Disclosures

- 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 component 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.
Scenarios
Question:

A PI receives health information from a HIPAA covered entity, but reports that the information is de-identified.

The only identifier of the individual is age. Is the PI correct?
Question:
A PI receives health information from a HIPAA covered entity, but reports that the information is de-identified.

The only identifier of the individual is age. Is the PI correct?

Answer:
No. The Privacy Rule lists identifiers of the individual or of relatives, employers, or household members of the individual, that must be removed as part of the de-identification process.

The definition of de-identified data requires the removal of age for all individuals over age 89 and all elements of dates indicative of age, except that ages and elements may be aggregated into a single category of age 90 or older;
<table>
<thead>
<tr>
<th>Question:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A PI receives health information from the Calumet Couple and Family Therapy Center. Is this information considered PHI?</td>
</tr>
</tbody>
</table>
Question:

A PI who is not a member of covered workforce, receives health information from the Calumet Couple and Family Therapy Center. Is this information considered PHI?

Answer:

No. the Calumet Couple and Family Therapy Center is not designated as a HIPAA covered component and the PI is not part of a covered entity, therefore, the health information maintained by this clinic is not PHI and not covered by HIPAA.

Check the list of Purdue covered components to determine whether a Purdue entity is covered by HIPAA.

http://www.purdue.edu/push/HIPAA/CoveredComponents/index.html
Question:

A PI, covered workforce of SLHS, is collecting personally identifiable health information from individuals for use in a study. Is this information PHI?
Scenarios

Question:
A PI, covered workforce of SLHS, is collecting personally identifiable health information from individuals for use in a study. Is this information PHI?

Answer:
Yes, personally identifiable health information collected by covered workforce, is PHI, when used for research. An authorization or waiver would be required.
Question:
A PI, workforce of the WL Psychology Treatment and Research Clinics, is collecting personally identifiable health information from individuals for use in a study. Is this information PHI?
A PI, workforce of the WL Psychology Treatment and Research Clinics, is collecting personally identifiable health information from individuals for use in a study. Is this information PHI?

Answer:
No. The PI is not covered workforce of a covered entity and individuals are not covered entities, therefore, the health information collected is not PHI.
Question:
A PI is receiving health information from an outside entity and states that no PHI is used. Is this correct?
**Question:**

A PI, not workforce in a covered entity, is receiving personally identifiable health information from an outside entity and states that no PHI is used. Is this correct?

**Answer:**

You should ask if the personally identifiable health information is received from a HIPAA covered entity. If the outside entity is not a covered entity, then the data is not PHI.
Question:
A PI is receiving health information from PUSH. The medical record number is provided with the health information given to the PI. Only PUSH staff have access to the health record system that ties a medical record number to an individual. All other identifiers of the individual have been removed. Is this information PHI?
**Question:**
A PI is receiving health information from PUSH. The medical record number is provided with the health information given to the PI. Only PUSH staff have access to the health record system that ties a medical record number to an individual. All other identifiers of the individual have been removed. Is this information PHI?

**Answer:**
Yes. Medical record numbers are included in the list of identifiers. If it is possible to identify a person using the information, the information is identifiable.
Question:
A PI is receiving the following information from the Purdue health plan about employees: department worked, sex, diagnosis, race. Is this information de-identified?
Question:
A PI is receiving the following information from the Purdue health plan about employees: department worked, sex, diagnosis, race. Is this information de-identified?

Answer:
No. It may be possible to determine the individual’s identity in a small department or by accessing claims data along with department demographical data. If additional information may be used along with the research data to identify a person, it is not de-identified.
A **HIPAA Liaison** has been assigned in each covered component to:

- act as the first point of contact for HIPAA questions,
- maintain the required documentation for that area,
- ensure that HIPAA training occurs, and
- ensure that policies and procedures are followed.

A list of all **HIPAA liaisons** at Purdue can be viewed at:

http://www.purdue.edu/push/HIPAA/Administration/files/hipaaliaisonroster.pdf

**Contact the HIPAA Liaison if:**

- You have any questions about research in a particular covered component.
- You receive a request for revocation of a HIPAA authorization related to data shared with a researcher by the covered component.

HIPAA policies, procedures and forms can be found at:

http://www.purdue.edu/hipaa/
HIPAA Privacy Compliance

If you have any questions or concerns about the privacy policies or their implementation in your department, please contact Purdue’s HIPAA Privacy Officer at:

hipaa-privacy@purdue.edu

For general HIPAA information, visit:
http://www.purdue.edu/hipaa
HIPAA Security Compliance is monitored by Purdue’s Chief Information Security Officer and designees.

Please contact ITaP Security and Policy if you are planning to:

- electronically transmit PHI,
- use removable devices for storing or accessing PHI (e.g. laptops, thumb drives, Ipad),
- are planning to store PHI at Purdue,
- have questions about securing electronic PHI.

ITaP Security and Policy, itpolicy@purdue.edu