Health Insurance Portability and Accountability Act of 1996

Tracking and Releasing Version

As of 3/14/2016
Medical Records Releasing and Tracking

✓ Compliance with HIPAA – Why is this important
✓ Penalties for Non-Compliance
✓ Access to and Requests to Provide PHI by the Patient or Their Legal Representative
✓ When Tracking of the Disclosure is Required
✓ General Requirements
Why is this important?

- Our patients trust us to take great care in the way we use and disclosure their confidential health information and trust us to comply with state and federal privacy laws.

- HIPAA enforcement provisions include civil and criminal penalties for non-compliance. Purdue has entrusted us to comply with the law.
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 is 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 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.
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 obtaining judgments on behalf of individuals for HIPAA violations.
Access to and Requests to Provide PHI by the Patient or Their Legal Representative
HIPAA requires that covered entities provide an individual or their representative the right of access to inspect and obtain a copy of their PHI, except:

- Psychotherapy notes; and
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Business Support Components at Purdue, business associates or their subcontractors or agents will refer individuals to the clinic that owns the record, to obtain record copies or to request that records are sent to a third party.

**Record Copies**

Staff trained and responsible for releasing health records at the clinic that provided the health care, will handle all requests for record copies, with a few exceptions, as stated in any clinic-specific releasing policy. Information disclosed by a provider to the patient, such as test results and other treatment discussions, are not considered “releases of records”.
Disclosures to Individual's Involved in Payment or Treatment

Verbal disclosures of PHI to the patient, their representative or individuals designated as participating in the individual's payment or treatment do not require an authorization but must be noted in the health or other record, as defined by department policy.

Prior to the disclosure of PHI to someone other than to the individual who is the subject of the information, the relationship of the person to the individual must be checked.

- Documentation of the patient or health plan member's indication of who is involved in their treatment or payment must be recorded in either a patient's health record, health plan member's system note or on the form "Designation of Individuals Who are Involved in My Payment or Treatment Decisions."

This documentation must be checked prior to disclosing information to a person when the patient or health plan member is not present. If the person is not listed in the documentation, the patient or health plan member can be contacted to verbally provide approval of the disclosure and the approval must be documented, when the disclosure is made, either in the health record or location as designated in departmental procedures.
Disclosures of Health Records to a Provider for Continuing Care
Medical records may be sent to a provider to whom a referral has been made for continuing care, without patient authorization but at request of the physician to whom the patient was referred. If an authorization is provided, the wishes of the patient must be respected whether or not a referral has been made. The disclosure must be tracked in the medical record.

Mental health records will be sent to referred providers for continuing care only with patient authorization or in an emergency situation. In the exceptional case where records are sent in an emergency without authorization, the disclosure will be tracked in the client's record.

When a patient or their legal representative requests records to be sent to another provider or a request is received from a provider where a referral has not been made by the clinic, a HIPAA authorization will be obtained from the patient to document the request and treatment relationship with the provider who is receiving the record.

In an emergency situation, records will be sent with verbal request by the patient or legal representative or a written request from the treating provider on the provider's letterhead and will be documented in the record.
Documentation of Request

Indiana State Law requires that requests for medical and mental health records be made in writing and Purdue generally, for medical records, and always, for mental health records, uses a valid HIPAA authorization to document these requests.

The Purdue HIPAA Privacy Office has provided an authorization form to be used for this purpose. The form can be found on the HIPAA website at: http://www.purdue.edu/hipaa in the Forms and Procedures section. If available, PHI may be directly accessible by the patient on a system portal, without documentation.
Quick Steps

When requests for access to or disclosure of PHI are received from a patient, health plan member, or their legal representative, the following steps should be followed:

<table>
<thead>
<tr>
<th>Step</th>
<th>Review Section for Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Identify the individual who is the subject of the information, Verification of Identity Requirements</td>
</tr>
<tr>
<td>2.</td>
<td>If applicable, identify the legal representative making the request, Legal Representatives</td>
</tr>
<tr>
<td>3.</td>
<td>If not on Purdue's form, obtain verification that the authorization is valid, HIPAA Authorization</td>
</tr>
<tr>
<td>4.</td>
<td>Determine the scope of disclosure, taking into consideration any restrictions or denial of access, Scope of Disclosure</td>
</tr>
<tr>
<td>5.</td>
<td>Determine the form or format in which the disclosure will be made, Form or Format and Electronic Copies</td>
</tr>
<tr>
<td>6.</td>
<td>Determine the method of disclosure, Method of Disclosure</td>
</tr>
<tr>
<td>7.</td>
<td>Comply with the disclosure timeframe requirements, Timeframe for Acting on Request</td>
</tr>
<tr>
<td>8.</td>
<td>Document the disclosure. Documentation of Disclosure</td>
</tr>
</tbody>
</table>
Disclosures of Test Reports

HIPAA provides an individual the right to access their information maintained by a HIPAA-covered laboratory, for as long as the information is maintained by the laboratory. This right extends to test reports and other information about the individual in a Designated Record Set maintained offsite, archived, or created before April 7, 2014.

- A HIPAA-covered laboratory is required to provide an individual with access only to that information that it actually maintains about the individual in the medical record at the time the request for access is fulfilled. Test reports are not considered to be part of the medical record until they are “complete,” when all results associated with an ordered test are finalized and ready for release.

- If the clinic utilizes an external laboratory for testing and the patient or their representative wishes to request test reports directly from the laboratory, the clinic will provide this contact information, upon request.

In certain circumstances, access to PHI may be denied in whole or in part. The denial of access will be documented by the provider in the medical record. Also, if the lab conducts anonymous testing and cannot properly identify the person, they are not required to give the results to the requesting individual.
Documented Request for Test Reports

A patient or their legal representative may request test reports from a laboratory in electronic or paper format. Indiana State Law requires that requests for copies of health records be made in writing.

- Patients requesting lab test reports will be asked to access the information directly in the patient portal, if available. If not available, if the patient refuses this option, or if a legal representative is making the request, the patient will be forwarded to the appropriate personnel trained to release health records and the request will be documented using a valid HIPAA authorization form.

- Requests for paper, electronic and transfers of information to another person or entity can also be securely completed by health record releasing personnel.
When Tracking of the Disclosure is Required
** Refer to the Disclosure Matrix in the Health and Mental Health Record Disclosures and Tracking procedures document.

- HIPAA requires tracking of certain disclosures of protected health information. Patients have the right to request a list of these disclosures that occurred during the 6 years prior to the request. The covered component’s health information management office, with assistance from the HIPAA Privacy Officer, is responsible for compiling the accounting of disclosures when requested by the individual. The HIPAA Privacy Officer will coordinate this effort and will respond to the individual when complete.

- Trackable disclosures do not require an authorization but must be tracked either on the Record of Disclosure form, on a form provided by the receiving entity (e.g. Indiana State Department of Health), as an entry in the patient health record or other system or file, as specified in departmental procedures.
Disclosures that are required to be tracked, include:

- Required by law (i.e. reports of animal bites),
- For judicial and administrative proceedings (i.e., Subpoenas, court orders, etc.),
- Certain disclosures for law enforcement purposes,
- Required for public health activities (i.e. reporting of disease to the Indiana State Department of Health),
- Required disclosures about victims of abuse, neglect or domestic violence,
- For reporting crime or for purposes of averting a serious threat to health or safety,
- 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),
- For health oversight activities (i.e. audits by an oversight agency),
- 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) (uses or disclosures that violate the Privacy Rule and/or minimum necessary standard).
Additionally, disclosures to persons other than to the patient will also be tracked in the medical or mental health record.

The information tracked for each disclosure will be:

- The date of the disclosure,
- The name of the entity or person who received the protected health information and, if known, the address of such entity or person,
- A brief description of the PHI disclosed, and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of the statement, a copy of a written request for a disclosure, if any.
If the covered component has made disclosures of PHI for a particular research purpose for 50 or more individuals, and where there has been a waiver granted by the IRB, the information tracked must include:

- The name of the protocol or other research activity,
- A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records,
- A brief description of the type of PHI that was disclosed,
- The date or period of time during which the disclosures occurred, or may have occurred, including the date of the last disclosure during the accounting period, and
- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed.

At the request of the individual, the covered component will assist the individual in contacting the entity that sponsored the research and the researcher.
Reports to the Department of Child Services of Suspected Abuse or Neglect

In accordance with applicable Indiana law, when Purdue or its clinics have a reasonable belief that a child is a victim of child abuse or neglect, the Clinic will make a verbal report to the Indiana Department of Child Services (DCS) or to local law enforcement.

- If Purdue makes an initial report of suspected child abuse or neglect, portions of the child's health record, necessary to provide evidence of the suspected abuse or neglect, may be provided upon request by DCS or local law enforcement, but only the minimum necessary records to provide evidence of the abuse will be released for this purpose. A physical exam, photographs or x-rays may be taken and provided, as needed, to support the verbal report. This disclosure does not require an authorization but must be tracked.
Requests for additional information or records, typically for follow up or other purposes, or any other information requested by DCS must be accompanied by a legal HIPAA-compliant authorization signed by the parent, guardian or legal custodian of the minor and, if applicable, guardianship documentation, or court order. In this case, an authorization or court order is provided and the disclosure does not need to be tracked.

DCS is required to obtain written authorization from the alleged victim’s parent, guardian, or custodian prior to obtaining:

- Any mental health assessment or treatment records,
- Any medical records for the alleged child victim that were not a part of the initial report from the provider, and
- Any alcohol use and/or substance abuse assessment or treatment records.

**Exception:** If the alcohol use/substance abuse records pertain to treatment that a minor who had the legal capacity to consent to such treatment received through his or her own voluntary consent, that minor is generally the only one who may consent to the release of the records, and he or she does not need additional consent of the parent, guardian, or custodian.

In cases where written authorization has not been provided, DCS must generally seek a court order authorizing the disclosure of information.
Disclosures to Foster Parents who are Under the Direction of DCS

Foster parents may obtain treatment for children who are under their care at Purdue’s clinics. They should be able to provide a letter from DCS that states that they have guardianship of the children and may obtain medical care.

Record Requests
Treatment notes and instructions related to the current visit can be given to the foster parents, however, additional medical records cannot be shared with the foster parents. The foster parents should be referred to DCS who can request medical records with either an authorization from the parents or a court order.

Provider Referrals
Requests for records to be sent to other providers for referral purposes should come only from DCS, not the foster parents. DCS will provide either a written parental authorization or a court order documenting guardianship.

http://www.purdue.edu/hipaa
hipaa-privacy@purdue.edu
Information Provided to Local Child Fatality Review Teams

If DCS requests information as a part of a Local Child Fatality Review Team, Purdue may release information requested by the Team in its official capacity. Purdue will require that all such requests be made in writing together with appropriate written verification that the request is being made by a duly constituted and appointed Local Child Fatality Review Team. In this case, the disclosure will be tracked.

** Should DCS question Purdue’s requirements for obtaining records, provide the letter titled: “Provision of Health Records to the Indiana Department of Child Services” to the requestor. The letter directs the recipient to contact Purdue’s HIPAA Privacy Officer if they have further questions.
Disclosures to a Coroner, Legal Requests or to a Health Oversight Agency

Disclosures to a Coroner or Medical Examiner
PHI may be disclosed to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. The disclosure can only be made to the coroner or medical examiner. If a law enforcement official calls requesting the information on behalf of the coroner or medical examiner, tell the official that you must speak to the coroner or medical examiner directly.

Disclosures to a Court of Law or Law Enforcement Official Pursuant to a Subpoena, Discovery Request or Other Lawful Process
Should a request for PHI be received by way of a subpoena, discovery request or other court document, the document will be sent to the campus Public Records Officer for validation. If the request is valid, the Public Records Officer will either make the disclosures herself or provide direction to the covered component about making the disclosure. When the PHI is delivered to the Officer, a copy of the legal document must be retained, typically in the patient health record and according to department procedures.

Disclosures to a Health Oversight Agency
Disclosures to a health oversight agency as requested in writing for health oversight activities, must be tracked in the patient health record or as specified in clinic procedures. The written request must also be retained.
Disclosures to law enforcement will be addressed as summarized, below. All of the disclosures below must be tracked.

**Required by Law:** As required by law, including laws that require the reporting of certain types of wounds or other physical injuries or as required by court order or court-ordered warrant, or a subpoena or summons. In the case of a court order, warrant, subpoena or summons, verify with University Counsel prior to disclosing.

**Decedents.** A covered component may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered component has a suspicion that the death may have resulted from criminal conduct.

**Crime on premises.** A covered component may disclose to a law enforcement official PHI that the covered component believes in good faith constitutes evidence of criminal conduct that occurred on the premises.
**Disclosures to Law Enforcement**

**Limited information for identification and location purposes.**
PHI may be disclosed in response to a law enforcement official’s request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that only the following information is given:

<table>
<thead>
<tr>
<th>Name and address;</th>
<th>Date and place of birth;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social security number;</td>
<td>ABO blood type and rh factor;</td>
</tr>
<tr>
<td>Type of injury;</td>
<td>Date and time of treatment;</td>
</tr>
<tr>
<td>Date and time of death, if applicable; and</td>
<td>A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.</td>
</tr>
</tbody>
</table>

The covered component **may not disclose** for this purpose any PHI information related to the individual’s DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

http://www.purdue.edu/hipaa
hipaa-privacy@purdue.edu
Disclosures to Law Enforcement

**Victims of a Crime:** A covered component may disclose PHI in response to a law enforcement official’s request for information about an individual who is or is suspected to be a victim of a crime, *only if:*

- The individual agrees to the disclosure; or
- The covered component is unable to obtain the individual’s agreement because of incapacity or other emergency circumstance, provided that:
  
  (A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
  
  (B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
  
  (C) The disclosure is in the best interests of the individual as determined by the covered component, in the exercise of professional judgment.
Reporting crime in emergencies. A covered health care provider providing emergency health care in response to a medical emergency, that occurred other than on the premises of the provider, may disclose PHI to a law enforcement official if the disclosure is necessary to alert law enforcement to:

- The commission and nature of a crime;
- The location of the crime or of the victim(s) of the crime; and
- The identity, description, and location of the perpetrator of the crime.

http://www.purdue.edu/hipaa
hipaa-privacy@purdue.edu
Disclosures about victims of abuse, neglect or domestic violence. Except for reports of child abuse or neglect, a covered component may disclose PHI about an individual whom the covered component reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

- To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of the law;
- If the individual agrees to the disclosure; or
- To the extent the disclosure is expressly authorized by statute or regulation and:
  (A) The covered component, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
  (B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
**Informing the individual.** A covered component that makes a disclosure about victims of abuse, neglect or domestic violence, must promptly inform the individual that a report has been or will be made, except if:

- The covered component, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

- The covered component would be informing a personal representative, and the covered component reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing that person would not be in the best interests of the individual as determined by the covered component, in the exercise of professional judgment.
Disclosures without authorization may be made to public health agencies, as required by law, for the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health agency.

**The Federal Drug Administration (FDA)**

A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

- To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
- To track FDA-regulated products;
- To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look back); or
- To conduct post marketing surveillance.
Requests for PHI from a researcher (not workforce of the covered component) for preparatory to research purposes (preliminary analysis or participant recruitment) must be made through the covered component's HIPAA liaison. **If the researcher is not a member of the covered component's workforce, a waiver must be granted from the IRB and the disclosures will need to be tracked.**

Researchers using PHI for preparatory to research purposes must agree that:

- Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
- No PHI is to be removed from the covered component by the researcher in the course of the review; and
- The PHI for which use or access is sought is necessary for the research purposes.

**Research on Decedent’s Information**

Requests by a researcher for research conducted using PHI about a decedent, will be made to the covered component's HIPAA liaison. The liaison will secure from the researcher a written:

- Representation that the use or disclosure sought is solely for research on the PHI of decedents;
- Documentation of the death of the individuals (e.g. death certificates); and
- Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.
General Requirements
**HIPAA Authorization**

**Only the Purdue version, or an authorization approved by the HIPAA Privacy Officer, is accepted.** A sample authorization indicating the information to be entered, is provided to ensure that information is correctly entered on the Purdue form.

- A copy of the signed document will be offered to the individual authorizing the disclosure. **Should the individual refuse a copy, the box will be checked at the bottom of the form stating, “☐ A copy of this form was offered and declined”**.

- The authorization will be maintained in the patient medical or mental health record, in the format as determined by the area HIPAA liaison, for 6 years after creation or effective date, whichever is later.

Individuals or their representatives may choose to revoke an authorization either before or after release of their PHI.
The authorization form received for request of record copies will be scanned into the patient's electronic health record or placed into the paper record, as applicable.

**Written Documentation of the Person Making the Disclosure**

In all cases where a written authorization or other written request for the release of medical or mental health records is obtained, the following information must be written on the clinic copy of the authorization and stored in the health record:

- the printed name and signature of the employee who disclosed the protected health information,
- the date the information was provided or sent,
- where the information was sent (e.g. mailing address, fax number, delivery in person), if not documented elsewhere on the authorization,
- the method of delivery, i.e. faxed, mailed, etc., and
- when a HIPAA authorization is signed by the patient or their representative in person, the staff member responsible for observing the signing of the form, must sign the “Witnessed” blank on the bottom of the form.

The last page of the Purdue authorization provides an area to record this information.
Revoking an Authorization

A request to revoke an existing authorization may be made in person and documented on the original authorization, or remotely in writing, and can be requested by either the individual who is the subject of the protected health information or their legal representative. If the request to revoke is made by the individual's legal representative, review the legal requirements for verification of an individual's status as a legal representative, prior to processing the request.

**Revocation Request Received in Person**

To revoke the authorization, the following information will be added to the authorization page where indicated on the second page of the Purdue form, or written where space allows on a non-Purdue form:

- date authorization revoked,
- check box to indicate "in-person revocation request",
- individual or legal representative printed name, relationship to individual (if not individual) and signature
- employee printed name and signature.

The word "REVOKED" must be written prominently across the front page of the authorization.
Revocation Request Received Remotely

To revoke an authorization remotely, the patient or their legal representative may provide a letter or use Purdue University's Request to Revoke Authorization form, found at:

Remote requests for revocations must be in writing and will be effective when processed by the covered component, not when written.

To process the revocation, the following information will be added by the department or clinic receiving the request, to the authorization page where indicated on the second page of the Purdue form, or written where space allows on a non-Purdue form:

- date authorization revoked (This is the date the revocation is processed.),
- check box to indicate "written revocation request-enclosed with authorization",
- individual or legal representative printed name, relationship to individual (if not individual) and signature
- employee printed name and signature.

The word "REVOKED" must be written prominently across the front page of the authorization.

If the written request for revocation is received remotely, a letter must be sent by the HIPAA liaison or their designee to the individual notifying them of the effective date of the revocation. A letter template is available at http://www.purdue.edu/hipaa/primary_menu/procedures_forms/general/index.shtml.
Modification of Authorization
If a request for modification of an authorization is received, the original authorization will be revoked and the individual will need to sign a new authorization form to execute the change.

Documentation of Request
The revoked authorization, letter or form requesting revocation, letter notifying patient of revocation, and any new authorizations, if applicable, must be retained in the health record.
Prior to any disclosure of PHI, a covered component must:

- verify the identity of a person requesting PHI,
- verify the identity of the patient, and
- the authority of the requestor to have access to PHI.

If the individual requesting health information cannot provide enough information to properly identify the individual, the covered component is not required to give the results to the individual requesting access.

**Patient Requests**

For all written requests for record copies, if the requestor is the patient, the following identifiers of the requestor must be provided either on a photo ID or provided verbally, if a photo ID is not available: *individual's name, PUID, and date of birth.*

*If no PUID is available, individual's name, date of birth, and local address must be provided.*

**These identifiers must be compared to the patient identity in the health record, prior to the disclosure of protected health information.**
Legal Representatives
The identity of the patient must be verified by the legal representative providing verbally: individual's name, PUID, and date of birth.

If no PUID is available, individual's name, date of birth, and local address must be provided.

To properly identify the legal representative and their authority to obtain an individual's PHI, a photo ID should be requested and must be compared against the identifiers on the documentation of legal representation, and in the case of a minor, the documentation of the identity of the minor's parents.

If a patient or health plan member is a minor, the names of parents must be collected at the time of patient registration.
Indiana State Law dictates who may act as a “personal representative” under HIPAA for an individual.

**Adult Patients**
An adult patient (generally someone who is 18 years old or older) may request medical information through a person acting as the person’s legal representative. These include someone who has been appointed as a power of attorney for the patient or an individual who has been appointed by a court to serve as the guardian of the patient.

An individual acting in the capacity of a power of attorney or a guardian must provide signed documentation of a representative’s ability to request records about an individual. Any questions about the documentation should be directed to the HIPAA Privacy Officer. A copy of the signed papers must be kept with the patient’s record and the legal representative must sign a release of information.
**Minor Patients**

Health records of a minor patient (generally someone who is under the age of eighteen years), may be requested by the minor patient’s parents, unless a guardian has been appointed for the minor patient. The names of the minor's parents or guardian should be requested on the form used to collect information about new patients. In general, minors may not request their own medical records except in the case where a minor is emancipated or consents to care as allowed under the law.

There are three situations when the parent would not be the minor's personal representative. These exceptions are:

- When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law. For example, if a minor has sought family planning services and wishes this information to be kept confidential, then a parent may not have access to this information,

- When the minor obtains care at the direction of a court or a person appointed by the court, such as when the minor has been placed in the custody of the Department of Family Services, or has a court appointed guardian ad litem or CASA and,

- When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

However, even in these exceptional situations, the parent may have access to the health records of the minor related to this treatment if the patient voluntarily consents to parental access.
Deceased Individual

Health Records

Health records of a deceased patient may be requested by a coroner or by the court appointed personal representative of the patient's estate. A personal representative will be able to provide a letter of administration (if there is no will) or a letter testamentary (if there is a will). A copy of this paperwork must be maintained with the signed authorization.

If the deceased individual does not have a court appointed personal representative, the surviving spouse of the deceased patient may make a request. If there is no surviving spouse, an adult child of the deceased patient or the parent, guardian, or custodian of the deceased patient’s child, if the child is a minor or not competent, may make a request. If the deceased individual is a minor child, then a parent or the parents may make a request for health information.

A valid HIPAA authorization, signed by the requestor of the records, must be provided to the clinic prior to the release of the records. If Purdue's authorization form is not used, the form must be approved by Purdue's HIPAA Privacy Officer.
Mental Health Records

Mental health records of a deceased patient may be requested by a coroner or by the court appointed personal representative of the patient's estate. A personal representative will be able to provide a letter of administration (if there is no will) or a letter testamentary (if there is a will). A copy of this paperwork must be maintained with the signed authorization.

If the deceased individual does not have a court appointed personal representative, the surviving spouse of the deceased patient may make a request. If there is no surviving spouse, any responsible member of the patient’s family, including a parent, guardian, or custodian of the deceased patient’s minor child may make a request. If the deceased individual is a minor child, then a parent or the parents may make a request for health information.

A valid HIPAA authorization, signed by the requestor of the records, must be provided to the mental health facility prior to the release of the records. If Purdue’s authorization form is not used, the form must be approved by Purdue’s HIPAA Privacy Officer.
Abuse, Neglect or Domestic Violence
The HIPAA Privacy Rule allows a covered component to elect not to treat a person as the personal representative of an individual if the covered component has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by the person, and the covered component, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual’s personal representative.
Scope of Disclosure

Only the information specified for release in the HIPAA authorization will be provided. Information that is legally restricted or subject to a denial of access will not be disclosed.

- If a letter accompanies the authorization and requests less information than authorized, the information requested in the letter will be provided.
- If the letter requests more information than is authorized, only the information specified in the authorization will be provided.

**Legal Restrictions**

- Information specified within an approved Request for the Restriction of the Use or Disclosure of PHI form or as documented by the health provider, will not be disclosed in compliance with the restrictions agreed to within that document. Approved restrictions must be documented in the patient medical or mental health record and the existence must be checked prior to disclosure.

The area HIPAA liaison will determine how the restriction or a denial of access will be documented, to ensure that staff are aware of and in compliance. The procedures for requesting a restriction can be found at: [http://www.purdue.edu/hipaa/primary_menu/procedures_forms/general/index.shtml](http://www.purdue.edu/hipaa/primary_menu/procedures_forms/general/index.shtml).
Denial of Access to PHI

The HIPAA Privacy Rule provides that a covered component may deny access to an individual to their PHI in certain situations and in some cases the individual may request review of the grounds for denial. Information determined by the patient's provider to be designated as "denied for access", must be documented in the health record according to clinic health or mental health record procedures.

Unreviewable Grounds for Denial

A covered component may deny an individual access, without providing the individual an opportunity for review, in the following circumstances.

- PHI maintained by a covered component that is: An individual’s access to PHI created or obtained by a covered health or mental health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered provider has informed the individual that the right of access will be reinstated upon completion of the research.

- An individual’s access may be denied if the PHI was obtained from someone other than a health or mental health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
Reviewable Grounds for Denial

A covered component may deny an individual access in the following circumstances, provided that the individual is given a right to have the denial reviewed.

- A licensed health care professional has determined, in the exercise of professional judgment, 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, in the exercise of professional judgment, 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 the personal representative is reasonably likely to cause substantial harm to the individual or another person.

Denial where the Grounds are Reviewable

In the case of a denial of access to PHI in whole or in part, the covered component must provide written denial to the individual, no later than 30 days after receipt of the request. The HIPAA Privacy Officer will draft this notice.

The denial must be in plain language and contain:

- The basis for the denial;

- If applicable, a statement of the individual’s review rights and a description of how the individual may exercise these rights; and

- A description of how the individual may complain to the covered component or to the Secretary of Health and Human Services. Purdue's HIPAA Privacy Officer is the person responsible for receiving HIPAA Privacy Complaints and who is able to provide further information about matters covered by the Notice of Privacy Practices.
Review of a Denial of Access.

If access is denied on a reviewable ground, the individual has the right to have the denial reviewed 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.

- After the review, the covered component must provide or deny access in whole or in part to PHI in accordance with the determination of the reviewing official, and to the extent possible, give the individual access to any other PHI requested.

- Requests to review a denial must be received from the patient or their legal representative in writing and provided to the HIPAA Privacy Officer. The HIPAA Privacy Officer will work with the clinic to designate the reviewing official and will coordinate a response to the patient.
**Timeframe for Acting on Request**

Covered components must act on a request for access to an individual's health information no later than 30 days after receipt of the request as follows.

- If the covered component grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested.
- If the covered component denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with *Denial of Access to PHI*.

If the request for access is for PHI that is not maintained or accessible to the covered component on-site, the covered component must take action to accept or deny the request but by no later than 60 days from the receipt of the request.

If the covered component is unable to take an action to accept or delay the request within the time required, as applicable, the covered component may extend the time by no more than 30 days, provided that:

- The covered component, within the 30 or 60 day time limit, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered component will complete its action on the request; and
- The covered component may have only one such extension of time for action on a request for access.
A covered component must provide the individual with access to the PHI in the

- form or format requested by the individual, if it is readily producible,
- or,
- if not, in a readable hard copy form or
- such other form or format as agreed to by the covered component and the individual.

**Summaries**

The covered component may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if:

- The individual agrees in advance to such a summary or explanation; and
- The individual agrees in advance to the fees imposed, if
- any, by the covered component for such summary or explanation.
Method of Disclosure

The method used to provide information to a recipient would include paper or electronic versions in person, US postal or campus mail, fax, electronic transmission.

The method of delivery must be secure and in compliance with the University Data Handling and Disposal Guidelines. Also, the HIPAA Communications and Office Security Guidelines should be referenced for information about securing PHI while in transit.

**Note that PHI may never be sent via unencrypted e-mail.**

Quick Reference

<table>
<thead>
<tr>
<th>Method of Disclosure</th>
<th>Security Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailed paper</td>
<td>Envelope (fill out To and From completely-do not mark confidential)</td>
</tr>
<tr>
<td>CD</td>
<td>Use encrypted CD</td>
</tr>
<tr>
<td>Electronic transmission</td>
<td>Use encryption tool, like FileLocker</td>
</tr>
<tr>
<td>Fax</td>
<td>Use a cover sheet filled out completely, and check the fax number, if necessary, to verify</td>
</tr>
</tbody>
</table>
Provision of Electronic Copies

If an individual requests an electronic copy of PHI that is maintained electronically in one or more Designated Record Sets, the covered health care component must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic format as agreed to by the covered component and the individual.

Covered components must provide individuals with some kind of readable electronic copy and images must be included, if requested. If the individual refuses the electronic copy that is readily producible, only then may a paper copy be provided. 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, if available.

Like all requests for record copies, the requests must be made in writing and through personnel designated and trained to release health records.

**CDs**

If the information is requested on CD, the covered component must copy the information onto an encrypted CD, provided by the University. Do not place a CD provided by the patient in your workstation drive as it could contain viruses. Contact the ITaP Security and Policy, itpolicy@purdue.edu, for encryption instructions.
**Electronic Transfer**
Individuals also may request that a covered component transmit an electronic copy of the PHI to themselves or another person or entity.

For electronic transmissions of PHI, HIPAA-covered components are required to comply with the HIPAA Security Rule, which requires encryption when transmitting electronic PHI.

*Many electronic health record systems provide secure messaging capabilities and the HIPAA Communication Guidelines or ITaP Security and Policy area can be referenced for acceptable alternatives, e.g. FileLocker.*

FileLocker instructions for use can be found at:
http://www.purdue.edu/hipaa/primary_menu/procedures_forms/data/FileLocker Instructions.pdf
The *Health and Mental Health Record Disclosures and Tracking* document is your reference for procedures to be used for disclosures of PHI.

Please read it and be familiar with the index on page 1 and the Disclosure Matrix on page 3. The Disclosure Matrix lists common disclosure types and whether an authorization or tracking is required.
HIPAA Officers

HIPAA Privacy Officer

As required by the HIPAA Privacy Rule, the individual responsible for the development and implementation of HIPAA policies and procedures for Purdue University and who is the primary contact for receiving complaints and is able to provide further information about matters covered by the Notices of Privacy Practices.

The Privacy Officer can be contacted at:

hipaa-privacy@purdue.edu

HIPAA Security Officer

As required by the HIPAA Security Rule, the individual responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule for Purdue University. The CISO serves as the University’s Security Officer.

The Security Officer is:

Greg Hedrick, x41875  hedrick@purdue.edu

Questions about securing e-PHI should be directed to ITaP Security and Policy, itpolicy@purdue.edu.

For general HIPAA information:  http://www.purdue.edu/hipaa