INDIANA UNIVERSITY

HIPAA-P05
Individuals' Rights under HIPAA

FULL POLICY CONTENTS

Effective: July 1, 2014
Last Updated: August 1, 2016

Responsible University Office:
HIPAA Privacy and Security Compliance Office

Responsible University Administrator
Vice President for Clinical Affairs

Policy Contact:
University HIPAA Privacy Officer

Scope

This policy applies to all personnel, regardless of affiliation, who create, access or store Protected Health Information ("PHI") under the auspices of Indiana University, designated for purposes of complying with the final provisions of the security and privacy rules regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Please refer to the HIPAA Affected Areas document for a full list of units impacted within Indiana University.

This policy addresses individuals' rights under the HIPAA Privacy Rule and applies to IU HIPAA Affected Areas (IU HAA) that are part of IU's health plans or direct treatment providers unless stated otherwise in the policy. For the purpose of this policy the health plan and direct treatment providers will be referred to as Health Care Components.

Reason for the Policy

Indiana University is committed to protecting the privacy of health information as required under the HIPAA Privacy and Security Rules. HIPAA affords individuals and their representatives certain rights, such as the right to receive a Notice of Privacy Practices and the right to access, inspect and copy their record or designated record set. This policy describes the rights afforded all individuals under the HIPAA Privacy Rule.

Policy Statement

I. Required Notice of Privacy Practices

A. General Rule

The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity's obligations with respect to that information. Most covered entities must develop and provide individuals with this notice of their privacy practices. IU Health Care Components must comply with the notice requirement.

B. Content of the Notice

Health Care Components are required to provide a notice in plain language that describes:

1. How the entity may use and disclose protected health information about an individual.
2. The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity.
3. The entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information.
4. Whom individuals can contact for further information about the Health Care Component's privacy policies.

The notice must include an effective date. See 45 CFR 164.520(b) for the specific requirements for developing the content of the notice. A covered entity is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices. See 45 CFR 164.520(b)(3), 164.520(c)(1)(i)(C) for health plans, and 164.520(c)(2)(iv) for covered health care providers with direct treatment relationships with individuals.

C. Providing Notice

1. The Health Care Component must make its notice available to any person who asks for it.
2. The Health Care Component must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits.
3. Health Plans must also:
    a. Provide the notice to individuals then covered by the plan no later than April 14, 2003 (April 14, 2004, for small health plans) and to new enrollees at the time of enrollment.
    b. Provide a revised notice to individuals then covered by the plan within 60 days of a material revision.
    c. Notify individuals then covered by the plan of the availability of and how to obtain the notice at least once every three years.
4. Covered Direct Treatment Providers must also:

a. Provide the notice to the individual no later than the date of first service delivery (after the April 14, 2003 compliance date of the Privacy Rule) and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.
b. When first service delivery to an individual is provided over the Internet, through e-mail, or otherwise electronically, the provider must send an electronic notice automatically and contemporaneously in response to the individual's first request for service. The provider must make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice.
c. In an emergency treatment situation, provide the notice as soon as it is reasonably practicable to do so after the emergency situation has ended. In these situations, providers are not required to make a good faith effort to obtain a written acknowledgment from individuals.
d. Make the latest notice (i.e., the one that reflects any changes in privacy policies) available at the provider's office or facility for individuals to request to take with them, and post it in a clear and prominent location at the facility.

5. A covered entity may e-mail the notice to an individual if the individual agrees to receive an electronic notice. See 45 CFR 164.520(c) for the specific requirements for providing the notice.

II. The Right to Access PHI

A. General Access

Under HIPAA, individuals have a right to examine and, if they wish, to receive a copy of, all the health information a covered entity has on an individuals that was used to make decisions about them. If an individual wishes to examine their health information or designated record set (DRS), each Health Care Component should have a process in place to allow them to do so.

If the patient wishes to examine their information held at other sites or multiple sites around campus such as their billing records, dental records, and chest x-ray images, the Health Care Component should provide them with a form designed for this purpose or refer them to the covered entity that houses their record (e.g., IUH - "Authorization to Release and Disclose Patient Information").

All requests for records must be accommodated within 30 days of the request. If an individual would like a copy of their PHI, the covered entity may charge a reasonable, cost-based fee for providing this. *Attachment A – Sample Request to Access*

B. Access to Mental Health Records/Access to Psychotherapy Notes

If an individual requests access to or copies of "psychotherapy notes", then the request may be declined if the provider determines there is a substantial risk of significant adverse or detrimental consequences to an individual in seeing or receiving a copy of mental health records requested by the patient. The only requirements are as follows:

1. The Health Care Component must make a written record and include it in the patient's file, noting the date of the request and explaining the provider's reason for refusing to permit inspection or provide copies of the records, including a description

of the specific adverse or detrimental consequences to the patient that the physician anticipates would occur if inspection or copying were permitted.

2. The Health Care Component must permit inspection or copying of the mental health records by a licensed physician, psychologist, marriage and family therapist, or clinical social worker designated by the patient. These health care providers must not then permit inspection or copying by the patient.
3. The Health Care Component must inform the patient of the provider's refusal to permit the patient to inspect or obtain copies of the requested records, and inform the patient of the right to require the physician to permit inspection by, or provide copies to, the health care professionals listed in the paragraph above. The provider must indicate in the mental health records of the patient whether the request was made to provide a copy of the records to another health care professional.

If an individual requests access to "mental health records" that do not qualify as psychotherapy notes (e.g., diagnosis and functional status summaries), the individual has the right of access to inspect and obtain a copy of the records, as long as the information is maintained in the DRS, unless an exception applies.

*C. **Exceptions to the individual's right to access***

1. Information compiled in anticipation of a civil, criminal or administrative action or proceeding;
2. Information not available because of restrictions under the Clinical Laboratory Improvements Amendments of 1988 (CLIA);
3. Oral communications;
4. The request is to a correctional institution or to the area under the direction of a correctional institution, if release of the information would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmate or an officer or employee of the correctional institution;
5. The PHI has been created or obtained by the IU HAA in the course of research that includes treatment and in the research consent process, the individual has agreed he or she will not be allowed access to that PHI so long as the research is in progress;
6. Information that is restricted by the Privacy Act; or
7. Information that was obtained from a third party other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to identify the source.

III. The Right to Amend PHI

*A. **Request to Amend Record***

An individual has a right to request that the Health Care Component amend the DRS or other information in the individual's record. The individual must provide a written request for the amendment and provide the reason to support the requested amendment. The Health Care Component must inform individuals in advance of these requirements (i.e., that the request for an amendment be in writing and that the individual provide a reason to support a requested amendment). The Health Care Component must maintain the written request for 6 years. *Attachment B – Sample Request to Amend*

B. ***Response to Request***

The Health Care Component must act on the individual's request for an amendment no later than 60 days after receipt of such a request by either accepting and making the amendment, or denying the request in writing. If the Health Care Component is unable to act on the amendment within 60 days, it may have a one-time delay of no more than 30 days by providing the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed within the initial 60 days of receipt of the request for an amendment.

1. Accepted Request to Amend

If the Health Care Component accepts the amendment in whole or in part, the area must:

a. Identify the affected records and link the amendment to the affected records in the DRS;

b. Inform the individual in a timely manner that the amendment has been made;

c. Obtain the individual's identification of and agreement to have the Health Care Component notify those persons with whom the amendment needs to be shared; and

d. Make a reasonable effort to notify those persons who the Health Care Component knows has the record that has been amended. These persons include those identified by the individual and others, including business associates, who should amend the record because reliance on the un-amended record could cause harm to the individual.

2. Denied Request to Amend

The Health Care Component may deny an individual's request for amendment, if it determines that the record:

a. Is accurate and complete without amendment;

b. Is not part of the designated record set;

c. Would not be available for inspection by the individual; or

d. Was not created by the Health Care Component, unless the individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment.

3. Notification of decision to Deny Request to Amend

If the Health Care Component denies the request to amend, they must provide in writing:

a. A denial written in plain language within the time limits described above;

b. A basis for the denial;

c. The process by which the individual may submit a written statement disagreeing with the denial, including the basis for disagreement and the Health Care Component's accepted length of the statement of disagreement;

d. A statement that if the individual does not submit a written statement of disagreement, the individual may request that the Health Care Component provide the individual's request for amendment and the written denial with any future disclosure of the PHI subject to the requested amendment; and

e. The process by which the individual may make a complaint to the Health Care Component or the Secretary, including the title, name, contact number of the appropriate Privacy Official.

IV. An Individual's Right to Request Restriction on the Uses and Disclosures of Protected Health Information (PHI)

A. Individuals have the right to request restrictions on: (a) how a covered entity will use and disclose protected health information about them for treatment, payment, and health care operations; (b) Disclosure of PHI to family members, friends, and others involved in their care.

A covered entity is not required to agree to an individual's request for a restriction, but is bound by any restrictions to which it agrees except as provided in 45 CFR 164.510(a)(1)(vi).

Each Health Care Component must have in place:

1. To allow an individual to request a restriction on disclosures of their PHI:
   a. for treatment, payment or health care operations;
   b. to family members, friends and others involved in their care
2. To accept or deny a request for restriction

B. A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

1. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
2. The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

Attachment C – Sample Request to Restrict

V. An Individual's Right to Request Confidential Communications

The Health Care Component must permit individuals to request communications of PHI from the area and must accommodate reasonable requests to receive communications of PHI by alternative means of communication or to alternative locations. The Health Care Component may not require the individual to explain the reason for the request.

The area will accommodate reasonable requests if:

A. Requests are made in writing to the responsible Health Care Component's designee with specific instructions as to location, address or fax number and include individual's signature and dated;

B. The request is for electronic communications via email or fax, and the individual has provided a signed request for electronic communications; and

C. The individual provides payment in advance for all costs of mailing to one or more alternative locations (e.g., FedEx, express mail, etc.) when the requests are for mailed communications, other than standard first class mail.

The Health Care Component shall document its response to any written request and maintain such documentation for six years following the last communication to which a request pertains.

VI. An Individual's Right to Request an Accounting of Disclosures

A. The Privacy Rule requires the Health Care Component to provide an individual with an accounting of the disclosures of the patient's PHI made by the Health Care Component in the six years prior to the date on which the accounting is requested except for the following uses and disclosures to or for:

1. The individual;
2. Treatment, payment and health care operations (note that if the covered component maintains all or part of the PHI in an Electronic Health Record (EHR) then the covered component eventually will be required to provide an accounting of disclosures for treatment payment or health care operations from the HER for up to 3 years to the date of the request.
3. Business Associates who have entered into either a Business Associate Agreement or Amendment as required, so long as the disclosure is for treatment, payment, or healthcare operations;
4. Incidental to treatment, payment and operations;
5. Authorized by the individual with a signed HIPAA authorization;
6. Part of a Limited Data Set disclosed under a Data Use Agreement, or of a De-identified Data Set;
7. The Facility Directory;
8. Persons involved in the individual's care, including others when the individual is present and to persons who should be notified of the individual's location, general condition or death;
9. Disaster relief purposes;
10. National security or intelligence purposes to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities authorized by the National Security Act;
11. Correctional institutions or law enforcement officials for custodial situations so long as the use or disclosure is for: the provision of health care, health and safety of the individual or other inmates or persons responsible for transporting inmates; law enforcement on the premises and for maintaining the good order of the correctional institution;
12. Health oversight or law enforcement agency who request temporary suspension of accounting because it may impede their activities (see documentation requirement); and
13. Those disclosures that occurred prior to April 14, 2003 or disclosures that were made more than 6 years prior to the date of the request for an accounting.

B. The individual must provide the Health Care Component with a written request for an accounting, and the Health Care Component must maintain the written request for six years.

C. The Health Care Component must respond to the written request for accounting within 60 days of receipt of the request. If the Health Care Component is unable to provide the accounting within 60 days, the Health Care Component is allowed a one-time delay of 30

days by providing the individual with a written statement of the reasons for the delay and the date when the Health Care Component will provide the accounting.

D. The Health Care Component must provide the individual with a written accounting that meets the following requirements:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed;
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of a written request for disclosure from an official source; and
5. If there have been multiple disclosures of the individual's PHI to the same person or entity for a single purpose, the accounting may include the information required for the first disclosure, date of the last disclosure and the number of disclosures made during the accounting period.

E. **Disclosures pursuant to a Waiver of Authorization**

1. Less than 50 individuals

The covered entity must account in each individual's record for disclosures of an individual's PHI pursuant to an IRB or Privacy Board Waiver of Authorization of the disclosure if the disclosure involves fewer than 50 individuals.

Attachment D – Sample Accounting (individual)

2. 50 or more individuals

If the disclosure of the individual's PHI is pursuant to an IRB or Privacy Board Waiver of Authorization and includes disclosures for a research purpose that involves 50 or more individuals, the Privacy Rule (45 CFR 164.528(b)(4)) provides for an alternate method of accounting for disclosures.

Attachment E – Sample Accounting (≥50)

F. An individual may request one free accounting of their disclosures in a rolling 12-month window. The Health Care Component may charge a reasonable cost-based fee for additional requests from the same individual within the 12-month window if the Health Care Component advises the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request in order to reduce or avoid a fee.

G. The Health Care Component must document and retain for 6 years:

1. The information required to be in the accounting;
2. The written accounting that is provided to an individual; and
3. The titles of the persons or officer responsible for processing accounting requests.

VII. Right to file a complaint

By law, health care providers (including doctors and hospitals) who engage in certain electronic transactions, health plans, and health care clearinghouses, (collectively, "covered entities") had until April 14, 2003, to comply with the HIPAA Privacy Rule. (Small health plans had until April 14, 2004, to comply). Activities occurring before April 14, 2003, are not subject to the Office for Civil Rights (OCR) enforcement actions. After that date, a

person who believes a covered entity is not complying with a requirement of the Privacy Rule may file with OCR a written complaint, either on paper or electronically. This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred. The Secretary may waive this 180-day time limit if good cause is shown.

Each Health Care Component should have a process in place to allow an individual to file a complaint as required under the HIPAA Privacy Rule. This process should be outlined in the notice of privacy practices as state in Section I. The Health Care Component should also provide the individuals with an opportunity to first file a complaint with the unit.

You must also inform the individuals you will not retaliate against them for filing a complaint.

A. ***Filing a complaint with Health Care Component***

Provide: Name of the Organization
Title of the Individual with whom they can file a complaint (Privacy Officer)
Write to: Address
City, State Zip
Call: Phone Number (as applicable)
Email: email address (as applicable)
Visit: Website (as applicable)

B. ***Filing a complaint with IU***

Provide: Indiana University
University HIPAA Privacy Officer
Write to: 980 Indiana Avenue, Suite 4438
Indianapolis, Indiana 46202
Email: HIPAA@iu.edu

C. ***Filing a complaint with the Department of Health & Human Services***

Provide: Department of Health & Human Services
Office for Civil Rights
Write to: 200 Independence Avenue, S.W.
Washington D.C. 20201
Call: 1-877-696-6775
Visit: www.hhs.gov/ocr/privacy/hipaa/complaints/

Definitions

See HIPAA Glossary for complete list of terms.

Forms

Attachment A – Sample Request to Access (IUH's Authorization to Release Records)

Attachment B – Sample Request to Amend

Attachment C – Sample Request to Restrict

Attachment D – Sample Accounting (Individual)

Attachment E – Sample Accounting (≥ 50)

Related Information

HIPAA-G01 – HIPAA Sanctions Guidance

HIPAA-P01	Uses & Disclosures of Protected Health Information Policy
HIPAA-P02	Minimum Necessary Policy
HIPAA-P03	HIPAA Authorizations

History

11/05/2013	Draft Revised and submitted to HIPAA Compliance Council
07/01/2014	Final
08/01/2016	Updated Definitions Section