INDIANA UNIVERSITY

HIPAA-A02
General Administrative Requirements

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 University Clinical Affairs

Policy Contact:
University HIPAA Privacy Officer
University HIPAA Security 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 IU HIPAA Affected Areas (IU HAAs) document for a full list of units impacted within Indiana University.

Reason for Policy

The reason for this policy is to ensure that the General Administrative Requirements under HIPAA are addressed and implemented.

Definitions

See Glossary of HIPAA Related Terms for a complete list of terms.

Policy Statement

Indiana University respects the privacy of all members of the IU community, and strives to implement measures to protect privacy consistent with the university mission and environment, applicable legal requirements and professional standards, generally accepted privacy norms, and available resources.

The provisions of this policy include the implementation of the following required components and documented policies and procedures:

I. Hybrid Status

Indiana University has designated itself as a Hybrid Entity as defined in the IU HIPAA Privacy Rule.

II. Notice of Privacy Practices

A. IU HAAs that are part of the IU health plans or are health care providers shall maintain a Notice of Privacy Practices that explains how they use and disclose (PHI), as well as an individual's rights and the IU HAA's legal duties under HIPAA.

B. The notice shall be written in plain language and shall include the terms required by HIPAA.

C. The IU HAA may not use or disclose PHI in violation of the Notice.

D. Except in an emergency situation, IU HAAs who are direct treatment providers shall do the following:

1. Make a good faith effort to obtain a patient's written acknowledgment of the Notice by the first date of service.
2. If the IU HAA is unable to obtain an acknowledgment, the IU HAA shall document the good faith efforts taken and the reason the acknowledgment was not obtained, if known.
3. In addition, the IU HAA shall post the Notice in a prominent location where it is reasonable for the public to see it, and shall make a copy of the Notice available upon request.

III. Safeguards

A. Administrative/Physical

1. IU HAAs shall have administrative and physical safeguards to protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of HIPAA.
2. IU HAAs shall reasonably safeguard protected health information to limit incidental uses or disclosures.
3. IU HAAs shall limit the protected health information access, used or disclosed to the minimum necessary to accomplish their goal.

B. Technical

1. IU HAAs shall periodically complete a *Risk Analysis* as required under the HIPAA Security Rule.
2. IU HAAs shall use the risk analysis to determine a *Risk Management* plan.
3. IU HAAs shall ensure all workforce who may use mobile devices to access PHI understand their responsibilities
4. IU HAAs shall ensure all workforce members understand their obligations to comply with IT 12.1 as applicable.
5. IU HAAs shall implement written policies and procedures to ensure these safeguards are in place.

IV. Training

A. IU HAAs shall train each new member of the workforce within a reasonable period of time (based on their role) after the person joins the workforce, but no longer than 90 days from the initial employment date.
B. IU HAAs shall require all workforce members to complete HIPAA Privacy and Security Training on an annual basis.
C. IU HAAs shall also train each member of the workforce whose functions are affected by a material change in the policies or procedures, within a reasonable period of time after the material change becomes effective.
D. IU HAAs shall document training has been provided to each member of the workforce and report to the University HIPAA Privacy Officer annually.
E. To support this policy, the IU HAA shall develop and implement a training program for the workforce members or offer the option of an approved E Training module.

V. Business Associates

A. Authorized members of the IU HAA workforce may disclose protected health information (PHI) to a business associate (BA), if the IU HAA has obtained satisfactory assurance that the BA will appropriately safeguard the information.
B. IU HAA may also permit a BA to create or receive PHI on the IU HAA's behalf.
C. The IU HAA shall document the satisfactory assurances through a written agreement with the BA that meets the requirements of the HIPAA Privacy Rule.
D. If the IU HAA becomes aware of a pattern of activity or practice of the BA that constitutes a significant failure to perform or a violation of the BA's contract, reasonable steps must be taken to cure the failure or end the violation. If such steps are unsuccessful, the contract shall be terminated. If termination is not feasible, the problem will be reported to the Secretary.
E. Activities of the Business Associates will be managed through the *Business Associate Agreement.*

VI. Limited Data Set

A. IU HAAs shall use data in the form of a limited data set when possible for the purposes of research, public health and health care operations.
B. IU HAAs will execute a Data Use Agreement or similar agreement when data are shared in the form of a limited data set, even when shared internally.

C. Data Use Agreements must be signed by the University HIPAA Privacy Officer as the authorized university official.

VII. Sanctions

A. IU HAAs shall follow IU's disciplinary policies including IU's Corrective Action Policy.

B. IU HAAs shall follow HIPAA-G01 *HIPAA Sanctions Guidance*.

Related Information

HIPAA Privacy and Security Rules

45 CFR §§ 160 and 164

HITECH Act - Amended

45 CFR §§ 160 and 164

Related IU Policies

HIPAA-G01	HIPAA Sanctions Guidance
HIPAA-P01	Uses & Disclosures of Protected Health Information Policy
HIPAA-P02	Minimum Necessary Policy
HIPAA-P07A	Designation of Indiana University as a Hybrid Entity
IT-12.1	IU Mobile Device Security Standard
PA/SS 6.4	Corrective Action Policy (non-union)
	University HIPAA Privacy and Security Compliance Plan
IRB SOPs	IU Standard Operating Procedures for Research Involving Human Subjects – Section 3.3.1.2 Limited Data Set

History

11/12/2013	Draft Sent to HIPAA Privacy and Security Compliance Council
07/01/2014	Final
01/12/2016	Updated Definitions Section
08/01/2016	Added link to Glossary