Indiana University HIPAA Privacy and Security Compliance Plan

Claire Tempel
Indiana University HIPAA Privacy Officer
August 8, 2019
Indiana University (IU) is committed to protecting the privacy and security of health information as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and applicable Indiana privacy and security laws. The Indiana University HIPAA Privacy and Security Compliance Plan (Plan) provides a framework that promotes understanding and compliance with these laws to ensure all IU workforce members are well informed of their responsibilities to maintain the privacy and security of patient, member, and/or subject data.

The objectives of the Plan are as follows:

1. Outline institutional, school and departmental compliance roles and responsibilities;
2. Establish policies and procedures to promote compliance with applicable federal, state and local laws, regulations and ordinances and communicate to the IU Workforce the policies and procedures all are expected to follow;
3. Develop and implement training to ensure the IU Workforce is aware of the required legal standards for HIPAA compliance and are updated in a timely manner on any changes in the standards or policies;
4. Develop and implement a means for IU Workforce to address questions and receive appropriate guidance regarding HIPAA issues;
5. Document and report IU HIPAA compliance, meetings, complaints, and investigations to the appropriate oversight bodies and leadership;
6. Establish a mechanism for individuals to report instances of non-compliance, so such reports can be fully and independently investigated;
7. Providing periodic reviews of overall HIPAA compliance efforts, including to verify practices reflect current requirements and to identify any necessary adjustments needed to improve compliance;
8. Pursuing corrective action to address any issues of non-compliance with HIPAA compliance polices and standards;
9. Coordinating compliance efforts with affiliates such as IU Health, IU Health Physicians, State of Indiana, Eskenazi Health and the Roudebush Veterans Administration Medical Center; and
10. Evaluate current use of protected health information (PHI) and identify other areas within the university engaged in HIPAA activities, and, where appropriate develop compliance initiatives.

A. Scope

IU is a covered entity that functions as a “hybrid covered entity” under HIPAA, meaning it is a single legal entity with components that are covered and non-covered under HIPAA. Areas that must comply with the HIPAA Privacy and Security Rules are known as IU HIPAA Affected Areas. IU HIPAA Affected Areas may have access to protected health information (PHI) because the area or unit: (1) is a covered healthcare component (healthcare provider or a health plan); (2) provides services to covered healthcare components or other covered entities and as such receives PHI to perform those services; or (3) uses PHI for education or research purposes.

This Plan applies to all IU Workforce Members, defined as employees, academic appointees, volunteers, trainees (including students, residents, and fellows), and other such persons who work under the direct control of an IU HIPAA Affected Area and who perform the functions, activities or services of either a covered entity or business associate, for and on behalf of Indiana University, as well as contracted third parties.

This Plan covers Indiana University’s responsibilities under the HIPAA Privacy and Security Rules and does not cover other HIPAA Rules, such as: Transactions and Code Sets, National Provider Identifier, Health Plan Identifier, Claims Attachments and other related rules (Other HIPAA Rules). The schools, departments, divisions and/or units impacted by Other HIPAA Rules shall be responsible for assessing the impact of these rules and for addressing compliance initiatives such as auditing and education of these non-privacy and non-security requirements.

The list of HIPAA Affected Areas and the IU Glossary of HIPAA Related Terms are located at compliance.iu.edu.
B. Privacy and Security Compliance Roles and Responsibilities

IU HIPAA Privacy and Security Officers

IU shall designate individuals to serve as the University HIPAA Privacy Officer and the University HIPAA Security Officer and provide sufficient authority to fulfill the duties inherent in those roles. The University HIPAA Privacy and Security Officers shall oversee, monitor, and coordinate compliance efforts university-wide with guidance from the IU Chief Privacy Officer and in collaboration with the University Information Policy Office (UIPO) and the University Information Security Office (UISO). The University HIPAA Privacy and Security Officers are accountable to the IU Chief Privacy Officer.

The University HIPAA Privacy and Security Officers shall coordinate with IU Affiliates to attempt to align IU and Affiliate policies and procedures, foster a community based upon trust and safeguarding PHI, assure workers are appropriately trained, and coordinate breach and security incident response, where appropriate.

IU HIPAA Affected Areas

IU HIPAA Affected Areas are responsible for implementing and monitoring their area’s compliance with the HIPAA Privacy and Security Rules, related state laws and IU policy, in collaboration with the University HIPAA Privacy and Security Officers.

HIPAA Affected Areas’ key responsibilities include, but are not limited to:

- Designate a representative responsible for HIPAA compliance to serve as a liaison to work with the University HIPAA Privacy and Security Officers;
- Develop a compliance plan, and work plan, as necessary, to pursue compliance with the HIPAA rules; report progress and issues to the University HIPAA Privacy and Security Officers;
- Assure appropriate policies and procedures are developed and implemented to address HIPAA privacy and security requirements and communicate information
(e.g. policies, procedures, guidance, etc.) regarding Workforce responsibilities in complying with HIPAA;

• Annually, track HIPAA required training for new and existing Workforce members and report compliance with the training requirement annually;
• Report privacy and security complaints and incidents in accordance with IU policy and coordinate resolution of breaches and security incidents with the University HIPAA Privacy and Security Officers;
• Maintain HIPAA documentation (e.g. area specific procedures, individual requests related to his or her PHI, log disclosures of PHI, training documentation, assessments and compliance plans) as necessary for compliance and reporting and retain documentation according to applicable regulations and IU policy.

C. POLICIES AND PROCEDURES

The University HIPAA Privacy and Security Officers shall lead the promulgation of reasonable and appropriate IU policies and procedures to comply with the provisions of the HIPAA Privacy and Security Rules, HITECH Act, and applicable Indiana privacy and security laws. The IU HIPAA policies and procedures shall be posted and available for all workforce members to easily gain access to the documents. Any change in IU HIPAA policies and procedures shall be communicated to the IU HIPAA Affected Areas for education and training.

IU HIPAA policies and procedures are posted at compliance.iu.edu.

D. EDUCATION AND TRAINING

All HIPAA Affected Area Workforce Members shall receive training related to the applicable HIPAA Privacy and Security Rule requirements and IU HIPAA policies and procedures, as necessary and appropriate to carry out their work functions. Training will include the overview of regulatory obligations and risks of non-compliance, as well as, specific requirements associated with administrative, physical and technical safeguards.

HIPAA training is required upon initial employment, volunteer work, student orientation, or third-party contract; and annually thereafter or upon material changes to any university or HIPAA Affected Areas’ policies and procedures.
regarding the privacy, security and confidentiality of individually identifiable health information (IIHI).

The University HIPAA Privacy and Security Officers shall be responsible for making available appropriate education and training opportunities to ensure policies concerning HIPAA compliance issues are disseminated and understood. The HIPAA Affected Area shall be responsible for ensuring all members of their workforce comply with this requirement as well as maintain documentation supporting compliance. Each HIPAA Affected Area shall provide an attestation annually to the University HIPAA Privacy and Security Officers and upon request will provide the supporting documentation.

Policy Reference:
HIPAA-P09 Education and Training for HIPAA Privacy and Security Awareness

E. COMPLIANCE AUDITING AND MONITORING

The University HIPAA Privacy and Security Officers, alone or in collaboration with IU Internal Audit, University Compliance, General Counsel, or others, shall identify and prioritize the HIPAA Affected Areas subject to compliance reviews. Auditing and monitoring may be conducted on a routine basis; in response to a special request; for cause following breaches, complaints or suspected non-compliance; or as part of corrective action.

Factors used to develop a compliance and monitoring audit plan may include, but are not limited to:
• Type of HIPAA Affected Area;
• OIG Work Plan;
• Prior non-compliance;
• Sensitivity of data;
• Likelihood of an exposure;
• Impact of an exposure;
• Extent of exposure to PHI, including the reason(s) for use & disclosure of PHI;
• Maturity or adherence to HIPAA Policies and Procedures;
• Compliance with training requirement;
• Types of Workforce Members (Roles);
• Methods of storage of PHI;
• Methods of sharing PHI;
• Number of individuals with access to PHI;
• Security Risk Assessment completed.

Auditing and monitoring activities may include, but are not limited to:
• Review of policies and procedures and other related documentation related to compliance with HIPAA Privacy and Security Rules;
• Conducting security risk assessments and developing management plans;
• Assessment of administrative, physical, and technical safeguards, including but not limited to assessing security of the physical site and safeguards for systems used to store, retrieve or share PHI;
• Assessment of training compliance.

If a review identifies issues of non-compliance, the University HIPAA Privacy and Security Officers shall work with the appropriate HIPAA Affected Area to rectify the issue(s). If necessary, The University HIPAA Privacy and Security Officers may consult the Office of the Vice President and General Counsel to determine if there has been any activity inconsistent with law or university policy. If, at the conclusion of any review, it appears there are compliance concerns, corrective action steps will be formulated and initiated on a timely basis.

**F. REPORTING SYSTEMS AND CORRECTIVE ACTION**

Indiana University maintains an “open door” policy with respect to information on suspected instances of non-compliance. IU Workforce are required to report any activity which they believe is in violation of the Plan, IU policy, or any regulatory requirement to the HIPAA Privacy and Security Officers. Failure to report knowledge of wrongdoing may result in disciplinary action up to and including termination. Any individual receiving a report of possible illegal or unethical conduct pertaining to the privacy and security of protected health information (PHI) must immediately advise the University HIPAA Privacy or Security Officer.

IU will not retaliate against any individual who reports in good faith actual or suspected violations of the laws, regulations, or policies. Although confidentiality cannot be guaranteed, all reported violations will be handled to ensure that the
identity of the reporting individual, and the person or persons involved in the suspected violation is only given to those persons with a need to know.

Indiana University shall maintain and publicize a Compliance Notification Line to be used to report compliance issues or possible violations of HIPAA or IU policy. To the extent possible, calls to the Compliance Notification Line at 888-236-7542 or via the web-link through EthicsPoint, will remain confidential and anonymous. The notification line will be operated in a manner designed to encourage complete disclosure by the caller giving information such as a particular description of the activity in question, the IU area in which it has taken place, and the identity of the people who may have knowledge of the relevant facts. A record will be maintained of any reports. Each reported concern pertaining to the privacy and security of protected health information (PHI) will be investigated by the University HIPAA Privacy and Security Officers.

Whenever conduct is discovered or reported that may be inconsistent with the Plan, IU policy or regulatory requirement, and if the University HIPAA Privacy and Security Officers determine a compliance issue may exist, they will make an inquiry into the matter following the IU incident response policy. As determined by the IU HIPAA Privacy and Security Officers, other areas such as Human Resources, Vice President for Faculty, or Dean of Students, may also be notified. IU Workforce shall fully cooperate with any inquiries undertaken by the University HIPAA Privacy and/or Security Officers.

The University HIPAA Privacy and Security Officers will prepare a recommended corrective action plan. In developing a corrective action plan; advice and guidance from the Chief Privacy Officer, the Dean of the appropriate school, a senior executive for that area, and the Office of the Vice President and General Counsel may be considered as appropriate.

Corrective action plans shall be designed to not only address the specific issue, but also take steps to avoid similar problems from occurring in the future. Corrective action plans may require changes to information handling and data protection practices, development or changes in policies and procedures, completion of training and other efforts to mitigate risks to privacy and security of Protected
Health Information (PHI). Sanctions or discipline, in accordance with university policies, may be recommended.

The University HIPAA Privacy and Security Officers or their designee shall maintain an incident log that records reports of privacy and security complaints and incidents, including the nature of any investigation and its results.

Policy Reference:
UA-04 Whistleblower Policy
ISPP-26 Information and Information System Incident Reporting and Management
ISPP-27 Privacy Complaints

Reporting Options and General Information

Members of the IU Workforce have various avenues to access additional information, request clarification or to report a compliance concern. IU Workforce Members are encouraged to discuss questions and concerns directly with their administrator, Chairperson or Dean, IU HIPAA Privacy and Security Officers, Chief Privacy Officer, or HIPAA Liaison.

Claire Tempel
Indiana University HIPAA Privacy Officer
ctempel@indiana.edu
hipaa@iu.edu
812-856-0340

Jason Bozarth
Indiana University HIPAA Security Officer
bozarthj@iu.edu
317-274-4281

IU Incident Response Team
It-incident@iu.edu
812-855-UISO (8476)
EthicsPoint Anonymous Reporting
888-236-7542
G. ENFORCEMENT AND DISCIPLINE

The aim of the HIPAA Privacy and Security Compliance Plan is to clarify the expectations of the IU community in order to achieve its goal of HIPAA compliant practices. Much of the conduct described herein is required by law and penalties for a violation can be severe for the University and IU Workforce Members. The implementation of the Plan is designed to pursue compliance with those standards. Enforcement of the Plan will follow the appropriate Indiana University disciplinary policy.

Policy Reference:
HIPAA-G01 Sanctions

H. REVISIONS TO THE PLAN

This Plan is intended to be flexible and readily adaptable to changes in regulatory requirements. This Plan should be reviewed to assess whether it is providing the desired results. The University HIPAA Privacy and Security Officers have the authority to amend this Plan as deemed necessary.

I. FEDERAL AND STATE REGULATIONS AND GUIDELINES

Indiana University must comply with applicable federal and state regulations and guidelines, the contract terms set forth by Business Associate Agreements or Data Use Agreements, and internal processes and policies to ensure compliance with the Plan.

These Regulations and Guidelines include, but are not limited to:
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Health Information Technology for Economic and Clinical Health (HITECH) Act, 2009
- Federal Policy for the Protections for Human Subjects, Common Rule: CFR Title 45, Part 46
- CFR Title 21 – Food & Drug Administration (FDA) Part 11
IU HIPAA Privacy and Security Compliance Plan

- 844 IAC 5-3: Article 5. Standards of Professional Conduct and Competent Practice of Medicine
- Indiana Code: 4-1-10: Chapter 10: Release of you Social Security Number
- Indiana Code: 4-1-11: Notice of Security Breach
- Indiana Code: 16-39-2-10: Descendents’ Records; Consent to Release
- Indiana Code: 16-41-8: Communicable Disease: Confidentiality Requirements

J. REFERENCES

- IU HIPAA Information, including policies, training resources, contact information, anonymous reporting, and other HIPAA related documents may be found at compliance.iu.edu
- Information on online safety and security, IT privacy and security policies, and how to report an incident may be found at protect.iu.edu
- Information regarding IU data management, data stewards, and the proper handling of IU Institutional Data may be found at datamanagement.iu.edu

- **Key IU Affiliates** include, but are not limited to:
  - IU Health - http://iuhealth.org/
  - IU Health Physicians - http://iuhealth.org/physicians/
  - Eskenazi Health - http://www.eskenazihealth.edu/
  - Indianapolis VA Medical Center - http://www.indianapolis.va.gov/
  - State of Indiana – Medicaid - http://www.in.gov/fssa/
  - State of Indiana - Public Health Department - http://www.in.gov/isdh/

K. HISTORY

- 01/28/2012 Final Document Published
- 01/30/2017 Updated URLs, Added Links (References), Removed Appendices
- 08/08/2019 Revised to reflect changes in organizational and programmatic structure

LAST REVIEWED: 08/08/2019