POLICIES AND PROCEDURES

HIPAA Compliance

ISUPP 13020

POLICY INFORMATION
Policy Section: *Governance/Legal*
Policy Title: *HIPAA Compliance*
Responsible Executive (RE): *General Counsel*
Sponsoring Organization (SO): *Office of General Counsel*
Effective Date: *September 19, 2022*
Last Reviewed: *N/A*
Next Review: *September 2027*

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates healthcare providers (Covered Entities) that electronically maintain or transmit Protected Health Information (PHI) in connection with a Covered Transaction. HIPAA requires each Covered Entity (CE) to maintain reasonable and appropriate administrative, technical, and physical safeguards for privacy and security. Entities or individuals who contract to perform services for a CE with access to Protected Health Information (Business Associates) are also required to comply with the HIPAA privacy and security standards.

II. DEFINITIONS

A. **Covered Entity:** Any health plan, healthcare clearinghouse, or healthcare provider that transmits PHI in electronic form in connection with a Covered Transaction.

B. **Covered Functions:** Functions that a Covered Entity performs which makes it a health plan, healthcare provider, or healthcare clearinghouse.

C. **Covered Transaction:** The transmission of information between two parties to carry out financial or administrative activities related to healthcare and includes: Healthcare claims or equivalent encounter information; healthcare payment and remittance advice;

coordination of benefits; healthcare claim status; enrollment and disenrollment in a health plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; healthcare electronic funds transfers (EFT) and remittance advice; or other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation.

D. **Electronic PHI (ePHI):** Any PHI that is maintained or transmitted in electronic media and may be accessed, transmitted, or received electronically.

E. **HIPAA:** The Health Insurance Portability and Accountability Act of 1996, as amended, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

F. **Hybrid Entity:** A single legal entity that conducts both covered and non-covered functions and designates Health Care Components in accordance with HIPAA.

G. **Health Care Component:** Any University school, department, program, clinic, or function that: (1) meets the definition of a HIPAA Covered Entity, if it were a separate legal entity; (2) performs Covered Functions; or (3) for purposes of this Policy is a Business Associate. These components will be designated by the Hybrid Entity in accordance with 45 C.F.R. 164.105(a)(2)(iii)(C).

H. **Protected Health Information:** Individually identifiable Protected Health Information transmitted by or maintained in electronic media or any other form of medium, excluding education records covered by the Family Education Rights and Privacy Act (FERPA) as amended, employment records held by the Covered Entity as an employer and information about a person who has been deceased for more than 50 years.

I. **Business Associate:** A University school department, program, clinic, or function that creates, receives, maintains, or transmits PHI to perform certain functions or activities on behalf of a University Health Care Component, or provides any function that involves the disclosure of PHI including but not limited to legal, accounting, consulting, management, administrative, or financial services.

J. **Breach:** The acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted which compromises the security or privacy of the PHI.

K. **Sanction:** Any corrective action taken following a violation of HIPAA or ISU's HIPAA Privacy policies or procedures.

L. **Workforce Members:** Employees, authorized volunteers, trainees, students, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity. This includes, for example, full-time, part-time, regularly scheduled contract workers, and members of the Board of Trustees.

III. POLICY STATEMENT

This policy sets forth the framework for ISU's Compliance with HIPAA. ISU is subject to the HIPAA regulations because certain units of the University are Covered Entities and Business Associates (BA). ISU has designated these Covered University Health Care Components (HCC) in ISUPP 1090 *HIPAA Hybrid Entity.* Each HCC is required to ensure CE compliance with safeguard and implementation specifications, and enforcement of CE and BA compliance with the HIPAA regulations. ISU has a designated HIPAA Compliance Officer to provide campus-wide leadership for HIPAA compliance.

IV. AUTHORITY AND RESPONSIBILITIES

Every employee in a covered component with access to ePHI is required to adhere to all HIPAA mandates. Violation of this policy may result in disciplinary action up to and including termination of employment. Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties of up to $250,000 per year and criminal Sanctions including fines and imprisonment.

The HIPAA Compliance Officer is responsible for creating and maintaining HIPAA policies and procedures for each of ISU's Health Care Components.

ISU's HIPAA Compliance Officer is authorized to develop and implement procedures for all Covered Entities at ISU and for those ISU departments that provide Covered Functions. These policies will be approved and updated by the HIPAA Advisory Committee. These policies and procedures will be updated timely to reflect any regulatory changes or updates.

The HIPAA Compliance Officer is also responsible for receiving and responding to complaints related to PHI; ensuring Workforce Members are trained appropriately; auditing workforce compliance with all policies and procedures; implementing Sanctions against Workforce Members; and for maintaining overall compliance with HIPAA regulations throughout all Health Care Components and those departments that perform Covered Functions.

The HIPAA Compliance Officer and the Chief Information Officer are responsible for the implementations of policies and procedures to ensure compliance with the HITECH Act throughout all healthcare.

ISU will maintain a HIPAA Advisory Committee (HAC) that is responsible for approving all procedures as it relates to the creation, storage, and transmission of ePHI or PHI within any ISU Covered Entity, or ISU department that performs any Covered Function. The HAC is composed of University employees whose area of responsibility directly relates to the oversight of the University's efforts to provide healthcare services in accordance with applicable laws and regulations. The HAC will meet at least monthly.

V. PROCEDURES TO IMPLEMENT

ISU's Health Care Component must:

A. Appoint a HIPAA compliance officer or officers.

B. Implement policies and procedures with respect to Protected Health Information that comply with HIPAA regulations including, but not limited to, ensuring compliance with and enforcement of PHI security, use and disclosure with other University employees as well as external third parties.

C. Maintain the policies and procedures it implements in written (paper or electronic) form.

D. Maintain a written (paper or electronic) record of actions, activities, or assessments required to be documented by the HIPAA regulations.

E. Retain such required documentation for six (6) years from the date when it was last in effect.

F. Implement a training program that informs all of the organization's staff, including management, of all policies and procedures that apply to them in their individual roles.

G. Inform patients of the Covered Entity's HIPAA policies, procedures, the patient's rights and responsibilities, and receive and maintain written acknowledgement of receipt of such information.

H. Promptly document and process any complaints of alleged HIPAA violations, mitigate any damages, investigate and address any violations.

I. Perform regular, ongoing monitoring, assessment, and revision, as necessary, to ensure continued compliance and enforcement of HIPAA standards.

J. Perform regular, ongoing monitoring, assessment and revision, as necessary, of HIPAA policies and procedures and documentation in response to environmental, operational, staff, technical, or legal changes including, but not limited to those aspects of the CE affecting the confidentiality, integrity, or availability of its PHI.

K. Workforce Members of ISU must adhere to the standards of HIPAA compliance and assume full personal and professional responsibility for maintaining those standards. This Policy applies to any Workforce Member or student in any course, internship, practicum, volunteer activity, or ISU sponsored activity, and other individuals who may be performing internships and/or volunteer activities in a healthcare facility or another Covered Entity under HIPAA as part of an ISU class in any of the University's Colleges, and will be enforced according to ISU's HIPAA policies and procedures.

L. Violations of the Policy by ISU Workforce Members or representatives will be handled by the HIPAA Advisory Committee and Human Resources.

M. It is the responsibility of each individual Workforce Member, faculty, and other employees such as internship coordinators to be able to recognize and refrain from any violation of the HIPAA privacy policy and to report observed violations. It is the responsibility of each student or Workforce Member to review all aspects of the course syllabus or other appropriate course documents relating to the course, program, internship, or other educational experience, including the HIPAA Privacy Policy. In doing so, Workforce Members acknowledge that they agree to adhere to these practices and procedures.

N. All violations of the ISU HIPAA privacy and security policies or procedures are taken very seriously. Violations will be reported to the HIPAA Advisory Committee to determine whether a violation has occurred, the extent of the violation, and appropriate Sanctions to be applied, where necessary. If a violation occurs in an outside facility separate and apart from the University, the appropriate parties there must be notified by the clinical preceptor/faculty or faculty of record. Faculty must report any violations to ISU's HIPAA Compliance Officer.

VI. RELATED LAWS, RULES, AND POLICIES

A. 45 CFR § 164.103

B. 45 CFR § 164.105

C. ISUPP 1090 *HIPAA Hybrid Entity*