

## **University Guidelines**

Section 14 Health Insurance Portability and Accountability Act (HIPAA) Hybrid Entity Designation

Issued: December 2024

Replaces:

---

### ***Background***

The HIPAA Privacy Rule, located at 45 C.F.R. Part 160 and Subparts A and E of Part 164, establishes national standards to protect individuals' medical records and other personal health information. It applies to SIU, in that SIU undertakes certain activities that render it a "covered entity," as defined below.

The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered functions (those functions the performance of which make it a covered entity) and non-covered functions to elect to be a "hybrid entity." To be a hybrid entity, SIU must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule and the Security Rule (located at 45 C.F.R. Part 160 and Subparts A and C of Part 164) will apply only to the health care components. If SIU did not make this designation, all of its operations would be subject to the HIPAA Privacy Rule and HIPAA Security Rule.

The Board of Trustees of SIU previously designated itself as a hybrid entity on April 10, 2003, and that designation was later updated on June 30, 2017. This document updates the SIU designation as a hybrid entity under the HIPAA Privacy Rule and supersedes all prior designations.

### ***Definitions***

Affiliate: A legally separate covered entity that has entered into a formal affiliation agreement with SIU in order to designate themselves as a single covered entity.

Business Associate: A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

Covered Entity: (1) A health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits protected health information in electronic form in connection with a "covered transaction."

Covered Transaction: The transmission of information between two parties to carry out financial or administrative activities related to health care, including health care claims or equivalent encounter information, health care payment and remittance advice, coordination of benefits,

health care 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, and health care electronic funds transfers and remittance advice.

Health Care Clearinghouse: An entity that processes nonstandard information it receives from another entity into a standard format, or vice versa.

Health Care Provider: A person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Plan: An individual or group plan that provides, or pays the cost of, medical care.

Individually Identifiable Health Information: Information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information: Individually identifiable health information (excluding, among other things, education records covered by the Family Educational Rights and Privacy Act (FERPA)) that is: (1) transmitted by electronic media; (2) maintained in electronic media; or (3) transmitted or maintained in any other form or medium.

Secretary: The Secretary of the U.S. Department of Health and Human Services or his or her designee.

### ***Institutional Safeguards***

SIU, as the HIPAA covered entity, will identify an enterprise-wide HIPAA Privacy Officer, who will design and implement appropriate policies and procedures to ensure that each health care component designated in this document complies with the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule, taking into account the size and the type of activities that relate to protected health information undertaken by each health care component. Specifically, he or she will ensure that:

- No health care component discloses protected health information to a non-health care component of SIU under circumstances in which the HIPAA Privacy Rule would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;
- Each health care component protects electronic protected health information with respect to another component of SIU to the same extent that it would be required under the

HIPAA Security Rule to protect such information if the health care component and the other component were separate and distinct legal entities; and

- If a person performs duties for both a health care component in the capacity of a member of the workforce of such component, and for another component of SIU in the same capacity with respect to that component, such workforce member does not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by the HIPAA Privacy Rule.

On behalf of SIU, the enterprise-wide HIPAA Privacy Officer, will be responsible for keeping and submitting such compliance reports as the Secretary may determine necessary regarding SIU's compliance with HIPAA, cooperating with the Secretary with respect to investigations or compliance reviews, and granting access to the Secretary to SIU's books and records that may be pertinent to ascertaining SIU's compliance with HIPAA.

The enterprise-wide HIPAA Privacy Officer will be responsible for ensuring that contracts or other arrangements with business associates meet the requirements of the HIPAA Privacy Rule and the HIPAA Security Rule.

### ***Health Care Components***

The following schools, departments, offices, or units of SIU are hereby designated as separate health care components of SIU, a covered entity under HIPAA.

- **SIU School of Medicine**

The following school and units will operate as a single health care component under the name of "SIU Medicine":

- SIU School of Medicine
- SIU Centers for Family Medicine (designated as a Federally Qualified Health Center)<sup>1</sup>

SIU Medicine will implement policies and procedures developed in conjunction with the Enterprise wide HIPAA Privacy Officer that outline how it will comply with the HIPAA Privacy Rule and HIPAA Security Rule. SIU Medicine will have a designated individual who will implement a HIPAA privacy program in consultation with the SIU enterprise-wide HIPAA Privacy Officer. SIU Medicine's designated individual will provide information necessary for reporting breaches as required by the HIPAA Breach Notification Rule and SIU policies and procedures to the Enterprise wide HIPAA Privacy Officer for reporting by the SIU covered entity. SIU Medicine will also have a

---

<sup>1</sup> SIU Physicians & Surgeons, Inc., as a separate legal entity, is not covered by this hybrid entity designation.

designated Security Officer who will implement a HIPAA security program. The designated individual and Security Officer may be the same individual.

- **SIU Carbondale**

The following components will operate as a single health care component under the name of “SIU Carbondale” (SIUC):

- SIUC Student Health Services/Center
- SIUC School of Allied Health Community Dental Center; and
- SIUC School of Allied Health Dental Sealant Grant Program;

SIUC will implement policies and procedures developed by the enterprise wide HIPAA Privacy Officer that outline how it will comply with the HIPAA Privacy Rule and HIPAA Security Rule. The SIU enterprise-wide HIPAA Privacy Officer will implement a HIPAA privacy program at SIUC. SIUC will provide information necessary for reporting breaches as required by the HIPAA Breach Notification Rule and SIU policies and procedures to the enterprise wide HIPAA Privacy Officer for reporting by the SIU covered entity. SIUC will also have a designated Security Officer who will implement a HIPAA security program.

- **SIU Edwardsville**

The following schools and units will operate as a single health care component under the name of “SIU Edwardsville” (SIUE):

- SIU School of Nursing We Care Clinic
- SIU School of Dental Medicine

SIUE will implement policies and procedures developed by the enterprise wide HIPAA Privacy Officer that outline how it will comply with the HIPAA Privacy Rule and HIPAA Security Rule. The SIU enterprise-wide HIPAA Privacy Officer will implement a HIPAA privacy program at SIUE. SIUE will provide information necessary for reporting breaches as required by the HIPAA Breach Notification Rule and SIU policies and procedures to the enterprise wide HIPAA Privacy Officer for reporting by the SIU covered entity. SIUE will also have a designated Security Officer who will implement a HIPAA security program.

***Business Associate Functions***

The departments or offices listed below, to the extent they perform covered functions on behalf of or in support of one or more of the health care components designated in this document, in the role of business associate if they were separate legal entities, are included in the designation of such health care components:

- The Office of General Counsel
- The Office of University Risk Management

- Internal Audit
- The Office of Information Technology
- The Office of Compliance and Ethics
- Department of Medical Records
- School of Medicine Human Resources Department
- Offices of Research Administration

### ***Enterprise Wide HIPAA Privacy Officer***

In addition to duties outlined in previous sections of this document, the enterprise-wide HIPAA Privacy Officer will have the following responsibilities:

- Developing and implementing policies and procedures related to HIPAA at the applicable health care component;
- Receiving and investigating allegations of violations of HIPAA;
- Evaluation of potential breaches of HIPAA;
- Determining whether an actual breach of HIPAA has occurred;
- Providing information necessary to comply with the HIPAA breach notification rule
- Conducting audits for HIPAA compliance when necessary;
- Providing HIPAA privacy-related education and guidance to the applicable health care components

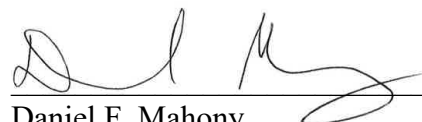
### ***Designated Security Officers***

For each health care component designated in this document, the HIPAA Security Officer identified for such health care component will be responsible for the following activities:

- Establishing, and the continuous management of, information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational information systems;
- Providing HIPAA security-related education and guidance to the applicable health care component;
- Conducting HIPAA security risk assessments;
- Identifying and responding to suspected or known security incidents.

### ***Record Retention***

This designation must be retained for six (6) years from the date of its adoption, or the date when it was last in effect, whichever is later.



---

Daniel F. Mahony  
President

12/17/2024

---

Date