~~HIPAA Privacy & Security Compliance Policy~~

~~**Background**~~

# ~~Congress enacted~~ HIPAA Privacy & Security Compliance Policy

## Policy Information

**Policy Owner:** (TBD – Possibly HIPAA Privacy and Security Official or Executive Director of University Ethics and Compliance)
**Approved by:** The Board of Trustees of the University of Illinois
**Date Approved:** 11/14/2013
**Effective Date:** 11/14/2013
**Date Amended (most recent): xx/xx/xxxx**
**Targeted Review Date: xx/xx/2020**
**Contact: hipaa@uillinois.edu**

## Purpose

This policy outlines the structure of the University of Illinois System's compliance program implementing the Health Insurance Portability and Accountability Act of 1996 ~~("HIPAA") to address the challenges presented by increasing reliance on electronic technology in health care. The Act charged the U.S. Department of Health and Human Services ("HHS") with establishing~~("HIPAA") and its companion regulations, including the HIPAA Privacy, Security, Breach Notification and Enforcement Rules (collectively "HIPAA Rules"). HIPAA and the HIPAA Rules establish national standards to protect the privacy and security ~~standards to be used when transmitting~~of protected health information ("PHI") and to promote standardized electronic transmission of common health ~~information electronically in connection with certain financial and~~ care related administrative and financial transactions. ~~These standards are known as the HIPAA Privacy Rule and the HIPAA Security Rule. HHS also adopted specific code sets used to identify diagnoses and procedures in electronic transactions.~~

## Scope

The University of Illinois System is a HIPAA ~~applies to *covered entities.* A~~ *covered entity* ~~is a health plan, a health care clearinghouse or a health care provider that transmits health information in electronic form in connection with specific financial and administrative transactions identified by HHS. Covered entities and their *business associates* must comply with the Privacy Rule standards to protect all individually identifiable health information held or transmitted by them in any form. This protected information is called *protected health information* ("PHI"). The Privacy Rule essentially prescribes who is authorized to access, use,~~

and disclose PHI, as well as the processes that must be in place in order to control the access, use, and disclosure of PHI.

Covered entities and their business associates also must comply with the Security Rule with respect to the covered entity's PHI in electronic form ("ePHI"). The purpose of the Security Rule is to ensure the confidentiality, integrity and availability of ePHI, to guard against security threats and to protect against unpermitted uses of ePHI..

This policy outlines the structure of the University's HIPAA compliance program implementing the Privacy and Security Rules.

**Who at the University is subject to the HIPAA Privacy & Security Rules**

The University of Illinois is a covered entity because certain of its units provide health care to the public and transmit health information electronically in connection with one or more HIPAA electronic transactions. The majority of the University'sSystem's units, however, aredo not health care providers that engage in HIPAA electronic transactions. perform HIPAA-covered functions. Consequently, the UniversitySystem has elected to self-designatedesignated itself as a *hybrid entity*. As a *hybrid entity*, the UniversitySystem may limit application of HIPAA to only those units or components of units that the University identifies as performingperform HIPAA- -covered functions. The units or components of the Universityunits identified as being covered by HIPAA are known as the *health care components* of the *hybrid entity*. The current list of the Systems' *health care components* can be found at http://go.uillinois.edu/hipaa.

This policy Units are labeled health care components either because they are health care providers that engage in electronic transactions or because they are *business associates.* A business associate is a person or contractor that creates, receives, maintains or transmits PHI on behalf of either a

~~HIPAA-covered entity or a health care component of a hybrid entity in performing a service or function for the covered entity or health care component. For instance, a University unit that requires PHI from a hospital to perform a service for the hospital, such as claims processing, data analysis, billing, legal, financial, consulting, data aggregation, management, or administrative services is a business associate of the hospital. That unit must be identified as a health care component of the University hybrid entity. A unit that is a business associate of a business associate also is subject to HIPAA and therefore must be designated as part of the health care component.~~

~~Members of the University's workforce within an identified health care component who perform either health care or business associate functions using PHI are subject to the Privacy and Security Rules and the relevant University policy requirements, including training. Workforce includes~~ applies to all employees, volunteers, trainees, ~~students~~ and other persons who work under the direct control of ~~the unit.~~

~~The health care components of the University hybrid entity as of the effective date of this policy are listed in Appendix 1. These units or components may change from time to time. The President will be responsible for ensuring the routine review and proper identification of the health care components by applying the Privacy Rule criteria.~~

~~**HIPAA Officials**~~

~~**President:** The President will oversee the University's HIPAA compliance program. As part of the oversight effort, the President will form a University-wide Privacy and Security Compliance Council ("Council") with the responsibilities set out below and will ensure that HIPAA Privacy and Security Officials are appointed as necessary.~~

~~**Privacy and Security Compliance Council:** The Council will serve in an advisory role. It will be chaired by the President or the President's designee and will include as members the Privacy and Security Officials, at least one representative from a health care component that provides health care services, at least one representative from a health care component that performs business associate~~ a *health care component* and who perform the functions, ~~a representative of the Office of University Counsel, a representative of the Office of University Audits, and such other individuals as the President deems appropriate. The Council will provide guidance and support to the University's HIPAA compliance program, assist Privacy and Security Officials as requested and report to the President, as appropriate~~activities or services of either a *covered entity* or *business associate*.

## Statement of Policy

The University of Illinois protects PHI by complying with the HIPAA Rules. To facilitate HIPAA compliance and to oversee the System's HIPAA compliance program, the President or his/her designee appoints a HIPAA Privacy Official~~: The President shall appoint one or more~~ and a HIPAA Security Official, who may be the same person. The HIPAA Privacy ~~Officials. If more than one~~Official and the HIPAA Security Official report to the President or his/her designee.

To facilitate HIPAA compliance by the *health care components*, each unit comprising one or more *health care components* will appoint a HIPAA liaison to coordinate with the HIPAA Privacy Official ~~is appointed,~~and the ~~President shall~~HIPAA Security Official. Units will designate additional HIPAA Liaisons from their ~~jurisdictions. The~~ health care components if requested to do so by the HIPAA Privacy ~~Officials will be~~ Official.

## Violations

Violations of the HIPAA Rules can lead to criminal and civil penalties for both the University of Illinois System and the individual(s) involved, as well as disciplinary action, up to and including separation of employment. Violations also can result in significant reputational damage.

## Procedures

The HIPAA Privacy Official and the HIPAA Security Official are responsible for the ~~development and implementation of~~following, coordinating and collaborating when required:

- In consultation with stakeholders, developing, approving, and implementing the policies and procedures required by the HIPAA ~~Privacy Rule. The Privacy Officials will regularly review~~Rules.
- Monitoring *health care component* compliance with the HIPAA Rules.
- Regularly reviewing the activities of System units to ensure ~~the~~ *health care components* are properly identified and ~~documented~~designated in writing~~; serve~~.
- Serving as a compliance resource to the *health care components*~~; develop and oversee~~.

~~HIPAA training and maintain related records; and monitor compliance with HIPAA. The Privacy Officials are authorized to receive, investigate, and recommend resolution of complaints concerning the University's compliance with the Privacy Rule, and they may convene a team of appropriate representatives to investigate reports of privacy breaches.~~

- **~~Security Officer:~~** ~~The President shall identify one or more HIPAA Security Officials. If more than one Security Official is appointed, the President shall designate their jurisdictions. The Security Officials will be responsible for the development and implementation of the policies and procedures required under the Security Rule. The Security Officials will establish and maintain administrative, physical~~Developing and maintaining HIPAA training and maintaining related records.
- Establishing and maintaining administrative, physical, and technical security safeguards to prevent, detect, contain, and correct security violations involving ~~ePHI. The Security Officials will cooperate with the Privacy Officials to monitor health care components for~~PHI in electronic form.
- Receiving, investigating, and recommending resolution of complaints concerning the System's compliance with the ~~Security Rule. The Security Officials are authorized to receive, investigate, recommend resolution and respond to alleged breaches of the Security Rule~~HIPAA Rules.

To facilitate HIPAA ~~**Liaisons:** Each~~ compliance within the *health care* ~~component will appoint a~~*components*, HIPAA ~~liaison. A liaison will have the following general responsibilities with respect to~~ liaisons, the ~~unit: identify members of the unit's workforce who engage in activities that involve use of PHI~~HIPAA Privacy Official and ~~ensure they are trained;~~the HIPAA Security Official shall cooperate ~~with~~in the ~~Privacy and Security Officials in~~ development ~~of~~and implementation of HIPAA policies and procedures and other compliance activities~~; and~~. HIPAA Liaisons serve as the point of contact for their respective health care components' questions, audits, and problem resolution ~~-~~regarding ~~the unit's compliance with HIPAA.~~HIPAA compliance, and identify workforce members of their respective *health care components* who engage in activities that involve use of PHI and ensure they are trained.

~~Date Approved: November 14, 2013~~

~~Authorities: HIPAA Privacy, Security and Enforcement Rules, 45 CFR Parts 160, 162 and 164, as amended through March 26, 2013~~

~~**Appendix 1:**~~

# Definitions

**"Business Associate"** means a person or entity that performs certain functions or activities on behalf of, or provides services to, a covered entity involving the use or disclosure of PHI. A covered entity can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities and particular services that make a person or entity a business associate, if the activity or service involves the use or disclosure of PHI. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. (45 CFR § 160.103)

**"Covered Entity"** means a health plan, health care clearinghouse or health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. (45 CFR § 160.103)

**"Health Care Component"** means a component or combination of components of a *hybrid entity* designated by the *hybrid entity* as component(s) that meet the definition of *covered entity* or *business associate* if such component(s) were separate legal entities. (45 CFR § 164.103; 45 CFR § 164.105(a)(2)(iii)(D))

**"Hybrid Entity"** means a single legal entity: (1) that is a *covered entity*; (2) whose business activities include both covered and non-covered functions; and (3) that designates its *health care components*. (45 CFR § 164.103)

# Training

All employees, volunteers, trainees, and other persons covered by this policy are required to receive appropriate HIPAA training. The HIPAA Privacy Official and the HIPAA Security Official may prescribe the content and frequency of the training subject to the requirements of HIPAA.

# Forms, Tools and Additional Resources

For more information about HIPAA at the University of Illinois ~~**Health Care Components**~~, visit http://go.uillinois.edu/hipaa.

| ~~University Administration~~ |
|---|
| ~~Office of University Counsel*~~ |
| ~~University Office of Risk Management*~~ |
| ~~Office of University Audits*~~ |
| ~~Administrative Information Technoloe:v Services (AITS)*~~ |

| |
|---|
| ~~University Ethics Office*~~ |
| **~~Chicago campus~~** |
| ~~University of Illinois Hospital & Health Sciences System~~ |
| ~~College of Applied Health Sciences~~ |
| ~~College of Dentistry~~ |
| ~~College of Nursing~~ |
| ~~College of Pharmacy~~ |
| ~~School of Public Health~~ |
| ~~College of Medicine at Chicago~~ |
| ~~College of Medicine at Rockford~~ |
| ~~College of Medicine at Peoria~~ |
| ~~Division of Specialized Care for Children*~~ |
| ~~Academic Computing and Communications Center (ACCC)*~~ |
| **~~Urbana campus~~** |
| ~~The School of Social Work*~~ |
| ~~Campus Information Technologies and Educational Services (CITES)*~~ |

~~* Those units with an asterisk perform business associate functions or services and are not health care providers.~~

## Website Address for this Policy

http://go.uillinois.edu/hipaa