HIPAA Privacy & Security Compliance Policy

Background

Congress enacted 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 national privacy and security standards to be used when transmitting health information electronically in connection with certain financial and administrative 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.

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's units, however, are not health care providers that engage in HIPAA electronic transactions. Consequently, the University has elected to self-designate as a *hybrid entity*. As a hybrid entity, the University may limit application of HIPAA to only those units that the University identifies as performing HIPAA-covered functions. The units or components of the University identified as being covered by HIPAA are known as the *health care components* of the hybrid entity.

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 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 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.

Privacy Official: The President shall appoint one or more HIPAA Privacy Officials. If more than one Privacy Official is appointed, the President shall designate their jurisdictions. The Privacy Officials will be responsible for the development and implementation of the policies and procedures required by the HIPAA Privacy Rule. The Privacy Officials will regularly review the activities of units to ensure the health care components are properly identified and documented in writing; serve 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 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 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 Liaisons: Each health care component will appoint a HIPAA liaison. A liaison will have the following general responsibilities with respect to the unit: identify members of the unit's workforce who engage in activities that involve use of PHI and ensure they are trained; cooperate with the Privacy and Security Officials in development of policies and procedures and other compliance activities; and serve as the point of contact for questions, audits, and problem resolution regarding the unit's compliance with HIPAA.

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:

University of Illinois Health Care Components

University Administration
Office of University Counsel*
University Office of Risk Management*
Office of University Audits*
Administrative Information Technology 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.