HIPAA Privacy & Security Compliance Policy

Policy Information

Policy Owner: HIPAA Privacy Official
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): 7/13/2017
Targeted Review Date: July 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") 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 of protected health information ("PHI") and to promote standardized electronic transmission of common health-care related administrative and financial transactions.

Scope

The University of Illinois System is a HIPAA *covered entity*. The majority of the System's units, however, do not perform HIPAA-covered functions. Consequently, the System has designated itself as a *hybrid entity*. As a *hybrid entity*, the System may limit application of HIPAA to only those units or components of units that perform HIPAA-covered functions. The units or components of units 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 applies to all employees, volunteers, trainees, and other persons who work under the direct control of a *health care component* and who perform the functions, 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 and a HIPAA Security Official, who may be the same person. The HIPAA Privacy Official and the HIPAA Security Official report to the President or his/her designee.

Commented [GDE1]: To clarify that health care components may consist of units or components of units that perform HIPAA-covered functions or activities, thus reducing risk by minimizing the number of individuals in the hybrid entity

Commented [GDE2]: To clarify that the President or the President's designee appoints the Privacy Official and the Security Official, who may be the same person, ensuring one point of accountability for privacy compliance and one for security compliance as required by law.

Commented [GDE3]: To specify that the Privacy Official and the Security Official report to the President or the President's designee, creating the necessary flexibility to establish the optimal HIPAA reporting structure

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 and the HIPAA Security Official. Units will designate additional HIPAA Liaisons from their health care components if requested to do so by the HIPAA Privacy Official.

Commented [GDE4]: The designation of the University-wide Privacy and Security Compliance Council has been removed from the policy given that its mandate is broader than HIPAA and it can be re-designated below the Board level

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 following, coordinating and collaborating when required:

- In consultation with stakeholders, developing, approving, and implementing the policies and procedures required by the HIPAA Rules.
- Monitoring *health care component* compliance with the HIPAA Rules.
- Regularly reviewing the activities of System units to ensure *health care components* are properly identified and designated in writing.
- Serving as a compliance resource to the *health care components*.
- 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 PHI in electronic form.
- Receiving, investigating, and recommending resolution of complaints concerning the System's compliance with the HIPAA Rules.

To facilitate HIPAA compliance within the *health care components*, HIPAA Liaisons, the HIPAA Privacy Official and the HIPAA Security Official shall cooperate in the development and implementation of HIPAA policies and procedures and other compliance activities. HIPAA Liaisons serve as the point of contact for their respective health care components' questions, audits, and problem resolution regarding 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.

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

Commented [GDE5]: To set forth the HIPAA training requirement for individuals covered by the policy

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, visit http://go.uillinois.edu/hipaa.

Website Address for this Policy

http://go.uillinois.edu/hipaa