Title/Subject: **HIPAA: ORGANIZATION FOR COMPLIANCE**

Applies to: ☒ faculty ☒ staff ☐ students ☒ student employees ☐ visitors ☒ contractors

Effective Date of This Revision: June 1, 2018

Contact for More Information: HIPAA Privacy Officer

☐ Board Policy ☒ Administrative Policy ☐ Procedure ☐ Guideline

---

PURPOSE:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) granted certain rights to individuals regarding their protected health information (PHI). This policy has been drafted to ensure a formalized HIPAA governance structure for CMU's effective management of compliance with applicable elements of the law and to guide CMU staff in assisting clients to exercise their rights.

POLICY:

1.0 **HIPAA Privacy Officer**. The president shall appoint a HIPAA Privacy Officer who shall be the designated official with centralized authority for HIPAA compliance and administration whose responsibilities are listed below. The HIPAA Privacy Officer shall report directly to the Chair of the HIPAA Executive Steering Committee, or other designee as appointed by the President, and shall have a direct communication line to the President.

1.1 Responsibilities:

1.1.1 Provides a coordinated university wide oversight of compliance with HIPAA, assuring that policies and procedures required to meet regulatory guidelines are developed and implemented in a timely manner.

1.1.2 Serves as HIPAA Privacy Officer for all covered entities at CMU; assures that applicable CMU units are kept informed about HIPAA requirements and developments.

1.1.3 Serves as chair of the HIPAA Compliance Council; assures that responsibilities of this council are coordinated so that persons best suited to complete tasks in each situation are assigned to those tasks; in cases of disagreement, makes decisions as to which representative and/or council subcommittee (in the case of sub-committee creations) shall be primarily responsible for certain tasks.

1.1.4 Oversees privacy and security compliance activities, working closely with HIPAA Representatives, HIPAA Council members, HIPAA Security Officer (see below), and HIPAA Executive Steering Committee (see below).

Authority: George E. Ross, President
History: 04-14-2003; 10-19-2006; 09-11-2017
Indexed as: HIPAA Privacy Officer, HIPAA Training Officer, HIPAA Complaint Officer, HIPAA Security Officer, HIPAA Compliance Council; HIPAA Organizational Chart

1.1.5 Signs off on all HIPAA related policy and procedure statements, including those which are specific to only one component of the CMU hybrid covered entity.

1.1.6 In coordination with the Office of General Counsel,

1.1.6.1 Provides guidance and assists in the identification, development, implementation and maintenance of uniform CMU HIPAA privacy and security policies and procedures.

1.1.6.2 Prepares uniform business associate agreements for outside vendors; develops the standard privacy policy to be used by each component of the hybrid covered entity.

1.1.6.3 Identifies designee or serves as member of, or liaison to, CMU's Institutional Review Board (IRB). Also serves as the information privacy liaison for users of clinical and administrative systems.

1.1.6.4 Maintains and applies current knowledge of applicable federal and state privacy laws and accreditation standards.

1.1.6.5 Serves as primary contact between the Office of Civil Rights, or other legal entities, and CMU officials in any compliance reviews or investigations for HIPAA related matters.

1.1.6.6 Establishes and administers a process for receiving, documenting, tracking, investigating and taking action on all complaints and reports of possible violations concerning CMU's HIPAA privacy policies and procedures.

1.1.6.6.1. Assures that CMU has effective policies and procedures for protecting individual from retaliation for exercising rights under HIPAA.

1.1.7 Assures consistent application of sanctions for failure to comply with privacy policies for all individuals in CMU's workforce and for all business associates, in cooperation with Human Resources, Faculty Personnel Services.

1.1.8 Develops and implements a schedule for regular review of HIPAA policies and procedures and also assures revisions to policies and procedures on an as needed basis.

1.1.9 Develops, implements, coordinates and prepares all required reports for the HIPAA Steering Committee's annual evaluation of the HIPAA program.

1.1.10 Collaborates with the Associate Vice President of Human Resource and Director of Benefits and Wellness to assure that all human resource related contracts applicable to HIPAA, have Business Associate Agreements established and are maintained in a centralized location within the CMU department of Human Resource Department.

1.1.11 Collaborates with the Director of Contracting and Purchasing and the applicable units to assure Business Associate Agreements are established by the units and also maintained in a centralized location within the CMU department of Contracting and Purchasing.

1.1.12 Supervisory and oversight responsibility for the HIPAA Training Coordinator.

2.0 **HIPAA Executive Steering Committee.** The President shall appoint the members of the HIPAA Executive Steering Committee whose responsibilities are listed below.

2.1 Composition:

2.1.1 Vice President for Research/Dean of Graduate Studies (Chair)
Executive Vice President/Provost
Vice President and General Counsel
Vice President for Information Technology/Chief Information Officer
Dean of College of Medicine
Dean of The Herbert H. and Grace A. Dow College of Health Professions

2.2 Responsibilities:

2.2.1 Provides executive level oversight of the HIPAA program through a formal annual evaluation process, developed in coordination with the HIPAA Privacy Officer.

2.2.2 Provides a consultant and leadership role to the HIPAA Privacy Officer in order to assure that he/she is able to carry out the duties of the HIPAA Privacy Officer including but not limited to the appropriate enforcement of HIPAA policies and procedures.

3.0 **HIPAA Representatives.** There shall be HIPAA Representatives that are responsible for serving as the appointees for their respective units that have been identified as a unit or department of the CMU HIPAA Hybrid entity. With the concurrence of the HIPAA Privacy Officer and HIPAA Executive Steering Committee, the appropriate vice president or College Dean shall appoint its HIPAA Representative.

3.1 Responsibilities:

3.1.1 Works directly with the HIPAA Privacy Officer in matters related to HIPAA on an immediate, ongoing, and as needed basis, including the assurance of timely reporting of breach incidents.

3.1.2 Assures implementation and compliance with HIPAA policies and procedures within their units.

3.1.3 Establishes process and site specific training for all staff within the unit who have access to PHI.

3.1.4 Assures Business Associate agreements (BAA) are established with all vendors to their units who are covered by HIPAA regulations, reviews language of the BAA with the HIPAA Privacy Officer and assures original BAA is maintained in the CMU department of Contracting and Purchasing.

3.1.5 Assures that HIPAA Privacy Notices are available and communicated as required by HIPAA.

3.1.6 Oversees patient and employee rights to inspect, request to amend, and restrict access to protected health information.

3.1.7 Assures that practices are in place to mitigate harmful effects of use or disclosure of protected health information in violation of CMU policies and procedures or requirements of law.

3.1.8 Serves on the HIPAA Compliance Council.

4.0 **HIPAA Training Coordinator.** The HIPAA Training Coordinator shall be appointed by and report directly to the HIPAA Privacy Officer.

4.1 Responsibilities:

4.1.1 Oversees, directs and delivers or ensures delivery of HIPAA training and orientation.

4.1.2 Oversees the maintenance of the HIPAA website and any HIPAA on-line training, coordinating with Information Technology and General Counsel.

4.1.3 Provides oversight of distribution of information about HIPAA and compliance requirements to employees, students, volunteers and others within the CMU community.

4.1.4 Initiates, facilitates and promotes activities to foster HIPAA awareness within CMU.

4.1.5 Maintains records of training completed by CMU workforce members within the CMU hybrid entity.

4.1.6 Provides secretarial duties to the HIPAA Privacy Officer and Compliance Council.

4.1.7 Assigns False Claims Act policy review and attestation to new hires and inter-department transfers into the HIPAA Hybrid entities. Monitors for timely completion as per the CMU False Claims Act policy.

5.0 **HIPAA Security Officer**. The HIPAA Privacy Officer and the Chief Information Officer will agree upon a person on the staff of the Office of Information Technology to be appointed HIPAA Security Officer.

5.1 Responsibilities:

5.1.1 Reviews all system-related information security plans throughout CMU's network to ensure alignment between security and privacy practices.

5.1.2 Assures compliance with electronic transaction standards.

5.1.3 Acts as liaison to the Office of Information Technology.

5.1.4 Monitors advancements in information privacy technologies to ensure CMU adaptation and compliance.

5.1.5 Coordinates establishment of systems, policies and procedures to comply with Security Regulations of HIPAA.

5.1.6 Serves on the HIPAA Compliance Council.

6.0 HIPAA Compliance Council

6.1 Composition:

6.1.1 HIPAA Privacy Officer (chair)
HIPAA Security Officer
HIPAA Training Coordinator
HIPAA Representative for each unit and/or clinical discipline of the covered entity
Director of Risk Management

Ad hoc as needed:
Units/departments within the non-healthcare components of the Hybrid Entity
HIPAA Executive Steering Committee members
Others may be asked to join as appropriate

6.2 Meetings:

6.2.1 Quarterly, minimum 4 times per year, and at call of the Chair.

(HIPAA Executive Steering Committee members shall attend the regular quarterly meetings as desired or as requested by the HIPAA Privacy Officer).

6.3 Responsibilities:

6.3.1 Serves as an active participant on the Council for conducting and documenting an ongoing HIPAA Risk Assessment, risk management, and corrective action.

6.3.1.1 Participates in ongoing and periodic review to assure that University has appropriate administrative, technical and physical safeguards for protected health information.

6.3.2 Works directly with the HIPAA Privacy Officer in matters related to HIPAA on an immediate, ongoing, and as needed basis and to include the assurance of timely reporting of breach incidents.

6.3.3 Develops and provides an annual report of HIPAA related activities to be presented to the HIPAA Executive Committee and the President. The HIPAA related activities in the annual report shall include but not limited to, HIPAA technical and non-technical risk assessment and risk management activities, HIPAA breaches, and changes in CMU environment or healthcare operations that results in a change to the healthcare components of CMU's hybrid entity designation.

6.3.4 Assures communication among all units of the University involved with HIPAA compliance; promoting university-wide personal responsibility and behaviors to ensure the privacy, security, and integrity of all sensitive information.

6.3.5 Engages in problem solving where broad input is needed.

6.3.6 Assures consistency in HIPAA related policies and procedures among components of hybrid covered entity.

6.3.7 Provides feedback on the successes and challenges of communication of HIPAA goals and rules to the campus at large.

6.3.8 Designates sub-committees as necessary.