To comment on this draft Policy, please click here.

University of Pittsburgh
Health Insurance Portability and Accountability Act
Policy AO [##]

Implementing Executive: Senior Vice Chancellor and Chief Legal Officer
Responsible Unit: Office of Compliance, Investigations, and Ethics
Category: Administration & Operations
Effective Date: [insert]

I. Purpose

This Policy establishes the responsibilities of University Members at the University of Pittsburgh ("University") under the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, as amended, and all federal regulations governing HIPAA implementation.

II. Scope

This Policy applies to all University units on all campuses determined to be Covered Components under HIPAA. This Policy also applies to researchers and independent contractors who are obligated to comply with HIPAA when they access, use, disclose, and/or create Protected Health Information ("PHI") during their scope of services to the University.

III. Definitions

A. Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a Covered Component. A member of the Covered Component's workforce is not a Business Associate.

B. Covered Component: An area within a Hybrid Entity that is a health care provider, health plan, or health care clearinghouse that transmits health information in electronic form in connection with a covered transaction. A Covered Component must comply with HIPAA.

C. Covered Transaction: The transmission of information between two parties to carry out financial or administrative activities related to health care (e.g. health claims, payment, coordination of benefits, enrollment or disenrollment, eligibility for a health plan, and other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation 45 CFR § 160.103).

D. Electronic Protected Health Information ("EPHI"): A form of PHI that is Individually Identifiable Health Information transmitted by electronic media or maintained in electronic media. Electronic Protected Health Information does not include education

records or treatment records covered by the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) or employment records held by the University in its role as an employer.

E. Health Information: is defined as any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and that is related to the past, present or future physical or mental health condition of an individual, the provision of health care of an individual, or the past, present or future payment for the provision of healthcare to an individual.

F. Hybrid Entity: An organization that performs both HIPAA-covered and non-covered functions as part of its business.

G. Individually Identifiable Health Information: is defined as any heath information, as defined above, that identifies an individual or where there is reasonable basis to believe that the information can be used to identify an individual.

H. Protected Health Information ("PHI"): Individually identifiable health information that is collected from an individual, created or received by a health care provider, health plan, health care clearinghouse, or other employee of one of the Covered Components of the University. This PHI is confidential and must be treated as protected under HIPAA. Protected Health Information 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.

I. University Member: All full-time and part-time faculty, staff, students, temporary employees, researchers, academic visitors, volunteers, postdocs, fellows, trainees, and interns at the University.

IV. Policy

A. Covered Components

The University is considered a Hybrid Entity under HIPAA. As a Hybrid Entity, the University Privacy Officer routinely identifies specific units to be Covered Components required to meet specific standards under HIPAA in the delivery of health care, paying for health care, and providing operational support for health care services. In addition, units providing services and support functions to those Covered Components involved in treatment, payment, and health care operations must meet specific requirements under HIPAA. A summary of the HIPAA privacy regulations is located at 45 CFR Part 160 and Subparts A and E of Part 164.

A list of the University's Covered Components may be obtained, upon request, from the Office of Compliance, Investigations, and Ethics at: compliance@pitt.edu .

Covered Components of the University and their individual University Members must comply with privacy and security practices in the use, storage, and disclosure of PHI as required by HIPAA and as set forth in University Procedure AO [insert #].

B. Training Requirements

University Members within a Covered Component of the University must receive training to assure their understanding of HIPAA privacy policies and procedures. This training must be appropriate for the members of the workforce to carry out their function within their employment, educational, or volunteering area. As part of their general employment orientation with the Office of Human Resources and/or the Office of the Provost, each new member of the Covered Components' workforce must also be trained on HIPAA privacy policies and procedures. In addition, all employees of the Covered Components must receive annual HIPAA training, including supplemental training updates when there is a substantial change in relevant privacy policies and/or regulations.

To ensure compliance with HIPAA training requirements, the University's HIPAA training and retraining will include, but will not be limited to, privacy and security training related to PHI. Additional training may be required for certain University Members to perform their specific job function in compliance with HIPAA.

Further information and guidelines on training requirements can be found here: https://www.compliance.pitt.edu .

C. Prohibition on Sale of PHI

University Members shall not directly or indirectly sell or receive payment in exchange for disclosing PHI unless either (a) the Covered Component obtains from the individual a signed valid authorization form from the University's Privacy Officer that specifically states their PHI can be further exchanged for payment, or (b) if the disclosure meets an exception as determined by the University's Privacy Officer and as set forth in the American Recovery and Reinvestment Act ("ARRA") Privacy Rule, as amended.

To request a valid authorization form or to request an exception for the sale of PHI, please contact the University's Privacy Officer at: compliance@pitt.edu .

D. Minimum Necessary Standard for the Use and Disclosure of PHI

PHI access and use shall be limited to only those University Members who need such access to carry out or perform their job responsibilities. Each University unit, department and School is responsible for appropriately limiting access to areas containing medical and confidential information. Only those University Members who need access to medical and confidential information in order to perform their work-related job responsibilities should have access to it and they should only have access to the minimum amount necessary.

All disclosures of PHI shall be limited to the amount reasonably necessary to achieve the purpose of the disclosure. Each Covered Component is responsible for ensuring that PHI is released as appropriate to or on behalf of patients or individuals.

For questions regarding administrative guidelines to ensure the confidentiality of PHI or the maintenance or disclosure of PHI for the purpose of treatment, payment and healthcare operations, research and education, or upon written consent, please contact the University's Privacy Officer at: compliance@pitt.edu.

Information that is requested must be limited to that information which is reasonably necessary to accomplish the purpose of the request. Reasonable efforts must be made to secure and maintain the confidentiality of PHI, regardless of form or media.

E. Visitors

Visitor access to patients and PHI shall be limited. Visitors shall be sponsored by an individual from a University management level position and shall be accompanied by a University staff member at all times during the visit. If a visitor is expected to come into contact with patients or PHI during the visit, the visitor shall sign a visitor confidentiality agreement. Should the visitor come into direct contact with a patient, the University staff member shall get approval from the patient prior to the visitor having contact with the patient.

A sample University Visitor Confidentiality Agreement is available upon request from the Office of Compliance, Investigations, and Ethics at: compliance@pitt.edu .

F. Security

Each Covered Component within the University is responsible for adopting site-specific procedures and controls to comply with HIPAA and all federal regulations governing HIPAA implementation as specified by the University's Chief Information Security Officer. Pitt IT and the Chief Information Security Officer shall have in place appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and availability of EPHI that is created, received, transmitted, or managed by the University's Covered Components.

Please refer to Procedure AO [insert #] for specific procedural requirements regarding security measures under this Policy.

G. Amendments to PHI

An individual may request an amendment to their PHI that is maintained by the University. Requests for amendment shall be made in writing and shall include a reason for requesting the amendment.

To request an amendment to PHI and for information on a Covered Component's responsibility on managing such requests, please refer to Procedure AO [insert #].

H. Notice of Privacy Practices

Each Covered Component shall provide a Notice of the University's Privacy Practices, which informs patients, faculty, staff and covered dependents as to how information about individuals may be used and disclosed, how the individual can obtain access to this information, and the individual's rights under HIPAA. For Covered Components that provide treatment, the Notice shall be provided to the individual at the time of registration and upon request. For the group health plan, Notice shall be provided automatically at the time of enrollment, upon request, and as required by the HIPAA Privacy Regulations. Each Covered Component shall make the Notice available on request to anyone and on their University website.

I. Use & Disclosure of PHI for Fundraising

PHI may be used or disclosed to a Business Associate for the purpose of raising funds to benefit the University provided the notice of privacy practices contains a statement that a University Member may contact the individual to raise funds for the University. Fundraising communications must contain clear instructions for how an individual can opt-out of receiving such communications in the future.

J. Use & Disclosure of PHI for Marketing

An individual's prior written marketing authorization is required to use or disclose PHI for marketing communications.

K. Complaints

The University Privacy Officer is responsible for the implementation and administration of an institutionally based complaint process in compliance with HIPAA.

Complaints arising under this Policy may be directed to the University Privacy Officer at: compliance@pitt.edu or to the Secretary of the U.S. Department of Health and Human Services if they believe their privacy rights have been violated.

V. Noncompliance

Failure to comply with the requirements of this Policy may result in sanctions in accordance with disciplinary policies or labor agreements applicable to University Members, including termination of employment. Students who fail to comply with the requirements of this Policy may be subject to sanctions in accordance with the Student Code of Conduct and/or Academic Integrity Guidelines, including dismissal from the University.

VI. Retaliation

No University Member may intimidate, threaten, coerce, discriminate against, or take retaliatory action against any person receiving health care or other services, or for exercising their rights under HIPAA.

VII. Governance and Responsibilities

A. **Office of Compliance, Investigations, and Ethics –** as requested by the Senior Vice Chancellor and Chief Legal Officer ("SVC-CLO"), responsible for implementing this Policy, including coordinating, and reviewing the University's overall compliance program and procedures relating to HIPAA as well as providing implementation support and resources. As part of this responsibility, and at the discretion of the SVC-CLO, the office may form ad hoc committees to support the University's HIPAA compliance program.

B. **University Privacy Officer -** responsible for coordinating compliance with specific standards of the HIPAA regulations at the University, including identifying University Covered Components and addressing complaints related to this Policy.

C. **Senior Vice Chancellor and Chief Legal Officer -** oversight responsibility for the implementation and monitoring of this Policy.

D. **Chief Information Security Officer –** as the University's HIPAA Security Officer, responsible for maintaining and overseeing privacy and security controls over University computer systems that store, transmit, or manage HIPAA data.

VIII. Contact Information and Public Accessibility

This Policy is posted under Administration & Operations Policies on the Office of Policy Development and Management's website and can be found at: https://www.policy.pitt.edu .

For specific questions related to this Policy, please contact the Office of Compliance, Investigations, and Ethics at: compliance@pitt.edu .

For specific questions related to research and compliance with this Policy, please consult: https://www.hrpo.pitt.edu/hipaa#WhatistheHIPAAPrivacyRuleandHowdoesitAffectResearchers

IX. Related Authorities

45 CFR Part 160 and Subparts A and E of Part 164
Secretary of the U.S. Department of Health and Human Services
University Procedure [insert #], HIPAA

To comment on this draft Policy, please click here.