University of Pittsburgh

HIPAA Compliance Program

Office of Compliance, Investigations & Ethics

Office of Compliance, Investigations & Ethics

Craig Hall, Suites 508-516
200 S. Craig Street
Pittsburgh, PA 15213

(412) 383-2766
compliance.pitt.edu

HIPAA COMPLIANCE PROGRAM

I. Introduction

II. Policy and Procedure

III. Identification of Covered Components, Business Associates, and PHI Workforce Members

IV. Component Responsibilities

V. Training

VI. Audits and Annual Reporting

VII. Complaints

I. Introduction

The Health Insurance Portability and Accountability Act of 1996, which may be amended from time to time, and including the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), collectively ("HIPAA"), requires the protection and confidential handling of protected health information ("PHI"), including electronic protected health information ("EPHI").

HIPAA establishes a set of national security standards for protecting certain health information, addresses the use and disclosure of individual's PHI/EPHI, and establishes standards for individual's privacy rights to understand and control how their PHI/EPHI is used. HIPAA also addresses the technical and non-technical safeguards used to secure PHI/EPHI.

The University is a Hybrid Entity, which means that only certain components (schools/departments/units) have operations to which HIPAA applies. A HIPAA Covered Component is an area of the University that serves as a health care provider, health plan, or healthcare clearinghouse that transmits health information electronically in connection with financial or administrative activities. These operations prompt compliance obligations under HIPAA for the component. The University has identified four Covered Components: The Office of Human Resources – Administration of Group Health Plan, Student Health Services and Pharmacy – Oakland Campus, The School of Dental Medicine, and University Dental Health Services.

University schools/departments/units that are not identified as a Covered Component may encounter PHI in their job functions, but they are not subject to HIPAA requirements. Employees and others within these schools/departments/units are called PHI Workforce Members. Though not subject to the same requirements as Covered Components, PHI Workforce Members are required to practice the safe handling and use of PHI.

Training for Covered Components and PHI Workforce Members regarding HIPAA's privacy and security rules, as well as the safe handling of PHI, personally identifiable information, confidential information, and education records pursuant to the Family Educational Rights and Privacy Act (FERPA) is an important part of this compliance program.

This program does not address PHI used or disclosed for research purposes. Obligations regarding PHI used or disclosed for research purposes are outlined on the Human Research Protections Office webpage.

II. Policy and Procedure

a. Definitions

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

Chief Information Security Officer (CISO): A senior-level University employee responsible for establishing and maintaining the enterprise vision, strategy, and procedures to ensure information assets and technologies are adequately protected, as well as the University's compliance with the HIPAA Security Rule. The CISO has delegated authority under Policy CS 30 to the University HIPAA Security Officer.

Component-specific HIPAA Privacy Officer: The component-specific Privacy Officer ("Component Privacy Officer") oversees all ongoing activities related to the implementation of, maintenance of, and adherence to the organization's policies and procedures related to HIPAA within their assigned Covered Component.

Component-specific HIPAA Security Official: The component-specific Security Official ("Component Security Official") is responsible for the ongoing management of information security policies, procedures, and technical systems to maintain the confidentiality, integrity, and availability of healthcare information systems within their assigned Covered Component.

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. These are the areas perform activities covered by HIPAA.

Designated Record Set: includes medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals.

Electronic Protected Health Information ("EPHI"): A form of PHI that is individually identifiable protected health information transmitted by electronic media or maintained in electronic media. EPHI does not include education records or treatment records covered by the Family Educational Rights and Privacy Act (FERPA), or employment records held by the university.

Health Information: 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.

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

PHI Workforce Members: workforce members and other parties at the University within schools, departments, or units that are not considered Covered Components, but may support our Covered Components or come into contact with PHI or EPHI over the course of carrying out their functions. Workforce members are not Business Associates; PHI encountered these areas is not covered under HIPAA but may still be protected by FERPA or other privacy laws.

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.

University Privacy Officer: A senior-level University employee responsible for managing compliance with information privacy laws and regulations, including compliance with the HIPAA Privacy and Security Rules.

University HIPAA Security Officer: A senior-level University employee to whom the CISO has delegated authority for compliance with the HIPAA Security Rule and other responsibilities under HIPAA.

Visitor: an individual who is not a patient, is not visiting a patient, or has no assigned duties at the University, or is not enrolled in a formal health related education program at the University. For example, a visitor may include, but not be limited to, a visiting physician, dentist, individual(s) touring a university facility, or undergraduates in a non-affiliated program who may be accompanying a physician or dentist during patient care activities, an employee of a University Business Associate or prospective Business Associate.

Visitor Sponsor: individual from a University management level position who shall have responsibility for the visitor(s) until the conclusion of their visit. Visitor Sponsors must adhere to the visitor guidelines in this program.

b. Key Provisions

i. Covered Components must comply with HIPAA and are expected to adhere to University Policies, procedures, and compliance program requirements.

ii. Access to PHI is limited to University Members who need access to carry out job responsibilities. All disclosures are limited to the amount reasonably necessary to achieve the purpose of the disclosure. Use of PHI for fundraising and marketing purposes, as well as the sale of PHI is limited.
iii. The University Privacy Officer is responsible for administration of the complaint process in compliance with HIPAA.
iv. Pitt IT and the University HIPAA Security Officer have administrative, technical, and physical safeguards in place to protect EPHI that is created, received, transmitted, or managed by the University's Covered Components. Safeguards include computer workstation and mobile device security. Covered Components are responsible for adopting site-specific procedures and controls. Site-specific procedures and controls should be developed in collaboration with the University Privacy Officer.
v. University's Covered Components shall, upon written request, provide to individuals an accounting of all disclosures of an individual's PHI.
vi. An individual may request an amendment to their PHI that is maintained by the University. Requests must be made in writing and include a reason for the amendment request.
vii. A Notice of the University's Privacy Practices shall be provided, 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.
viii. Training requirements apply to employees of all Covered Components, Business Associates, and PHI Workforce Members.
ix. Visitor access to patients and PHI should be limited. Visitors and visitor sponsors must complete required documentation prior to visit occurring.

III. Identification of Covered Components, Business Associates, and PHI Workforce Members

a. Covered Components

Covered Components are areas within the University that serve as a healthcare provider, health plan, or health care clearinghouse that transmits health information in electronic form in connection with a covered transaction. "Health care providers" include providers of health or medical services, such as hospitals, physicians, dentists, and other practitioners, as well as any person or organization that furnishes, bills, or is paid for healthcare in the normal course of business.

The University has identified the following Covered Components:

Office of Human Resources – Administration of Group Health Plan
Student Health Services and Pharmacy – Oakland Campus
The School of Dental Medicine
University Dental Health Services

b. Business Associates

A Business Associate is a person or entity that is contracted to perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a Covered Component. A member of a Covered Component's workforce is not a Business Associate. Covered Components are responsible for the development and implementation of Business Associate agreements, which must be approved by the University Privacy Officer and Office of University Counsel.

A list of all HIPAA Business Associates is available upon request from the Office of Compliance, Investigations and Ethics (CIE).

The preference of the University is to use the University of Pittsburgh Business Associate Agreement. Any modifications or proposed changes to the same must be approved by the University's Privacy Officer and the Office of University Counsel.

All requests to execute external Business Associate Agreements must be approved by University Privacy Officer and Office of University Counsel.

c. PHI Workforce Members

PHI Workforce Members are employees and other parties at the University within schools, departments, or units that are not considered Covered Components but may encounter PHI or EPHI over the course of carrying out their functions. PHI Workforce Members are expected to safely handle PHI and other sensitive information, while maintaining confidentiality and security. PHI Workforce Members will receive training on these topics as part of this program.

IV. Covered Component Responsibilities

Covered Components are expected to adhere to each of the following standards and guidelines outlined in this program. Documentation referenced throughout this compliance program should be retained for the period designated by the records retention schedule applicable to the Covered Component.

a. PHI Privacy

The University Privacy Officer shall oversee all ongoing activities related to the development, implementation, and adherence with this compliance program. The

University Privacy Officer, University HIPAA Security Officer, Component Privacy Officers, and Component Security Officials will work collaboratively to ensure HIPAA compliance.

Covered Components must:

i. Identify a component-specific HIPAA Privacy Officer, who shall, within their assigned component:

Ensure Covered Component's full coordination and cooperation under University HIPAA policies and procedures and legal requirements. For more detailed descriptions of the procedural requirements please see Guidance for Component Privacy Officers.

Ensure that Covered Component utilizes the appropriate forms, notices, and materials relating to current University HIPAA policies and procedures.

Perform periodic privacy risk assessments and conduct compliance monitoring activities in coordination with the Pitt IT Security and CIE Office.

Oversee, direct, deliver or ensure delivery of initial and ongoing HIPAA and privacy trainings for component employees, Business Associates, and other appropriate third parties.

Participate in the development and implementation of Business Associate agreements and monitor compliance with these agreements.

Serve as Covered Component's Case Manager in Pitt Concern Connection for all HIPAA-related concerns associated with the Covered Component.

Cooperate in any compliance reviews or investigations.

ii. Nominate a component-specific HIPAA Security Official, who, after approval of the nomination is received by the Pitt IT Security Office, shall, within their assigned component:

Implement, manage, and enforce information security directives as outlined in University HIPAA policies and procedures and in conjunction with Pitt IT Security. For more detailed descriptions of the procedural requirements please see Guidance for Component Security Officials.

Develop procedures to document responses in writing, including remediation steps, for lapses in compliance to University HIPAA Security Officer.

Ensure that the access control, disaster recovery, business continuity, incident response, and risk management needs of the component are properly addressed.

Perform ongoing information risk assessments and audits, in conjunction with Pitt IT Security, to ensure that information systems are adequately protected and meet all requirements.

b. PHI Security

The security of Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) requires annual technical security assessments of potential risks and vulnerabilities relating to confidentiality, integrity, and availability of PHI and EPHI. Periodic security updates will be provided by Pitt IT Security.

Covered Components must:

i. Ensure the Component Security Official documents responses, including remediation steps, for lapses in compliance and sends them to the University HIPAA Security Officer in writing.
ii. Complete the Annual Technology Security Assessment – In coordination with Pitt IT Security.
iii. Complete regular Records Reviews, including system activity records and compliance reviews.
iv. Implement Incident Response Procedures which include notification of the Component Security Official and a business continuity plan.
v. Ensure that all vendors undergo a vendor security review conducted by Pitt IT Security

c. Notices

Notice of the University's Privacy Practices, which inform 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 must be provided.

Covered Components must:

i. Provide Notice of University Privacy Practices available by request to anyone and publish the notice on their university website.
ii. *(For components that provide treatment)* Provide Notice of University Privacy Practices at the time of registration and upon request.

iii. *(For the group health plan)* Provide Notice of University Privacy Practices automatically at the time of enrollment, upon request, and as required by HIPAA Privacy Regulations.

d. Disclosure Accounting

University's Covered Components shall, upon written request, provide to individuals an accounting of all disclosures of an individual's PHI.

Covered Components must:

i. Track disclosures of PHI
ii. Establish component-specific procedures for responding to Disclosure Accounting Requests

    Responses to disclosure requests must include applicable disclosures made to or by Business Associates of the Covered Component

iii. Establish procedures for responding to Disclosure Accounting Requests for specific Business Associates

    A requestor may contact a Covered Component to request disclosures from a Business Associate of that component, or may contact a Business Associate directly to request an accounting of the disclosures of their PHI.

e. Use and Disclosure of PHI: Fundraising

PHI may be used or disclosed to a Business Associate for fundraising purposes if the notice of privacy practices contains a statement that the university can contact individuals to raise funds.

Covered Components Must: Ensure that fundraising communications contain clear instructions for how an individual can opt-out of such communications

f. Use and Disclosure of PHI: Marketing

An individual's prior written marketing authorization is required to use or disclose PHI for Marketing Communications. This authorization expires when the individual is no longer an established patient or can be revoked at any time via written request.

Covered Components Must: Ensure that consent in writing has been obtained from the individual prior to using or disclosing PHI for marketing communications

g. Use and Disclosure of PHI: Sale of PHI

The sale of PHI is prohibited without prior authorization by the University Privacy Officer.

Covered Components must: Ensure that proper permissions and documentation have been obtained from the University Privacy Officer prior to engaging in the sale of PHI.

h. Amendments to PHI

Individuals may request, in writing, an amendment to their PHI maintained by the University.

Covered Components must:

i. Respond to amendment requests within 60 days of receiving the request

   One 30-day extension is permitted if the Covered Component provides the requestor with a written statement of the reasons for delay and the date by which the Covered Component will complete the request.

ii. Report all requests for amendments to PHI to the Office of Compliance, Investigations and Ethics
iii. Establish component-specific procedures for approval and denial of amendment requests
iv. Issue amendment approval or denial letters to requestors as appropriate

i. Visitors

Visitor access to patients and PHI shall be limited.

Covered Components must:

i. Ensure that visitors are sponsored by an individual from a university management position
ii. Ensure that visitors are always accompanied by the Visitor Sponsor or a University staff member during the visit
iii. Visitor Sponsor should provide visitor(s) with instructions regarding privacy considerations and behavioral expectations prior to visit
iv. If a visitor is expected to come into contact with patients or PHI during the visit, Visitor Sponsor must ensure that the visitor signs a confidentiality agreement prior to beginning visit activities
v. If a visitor comes into direct contact with a patient, the Visitor Sponsor or accompanying University staff member shall obtain approval from the patient prior to the visitor having contact with the patient

j. Destruction of PHI

Records containing PHI should be destroyed according to the component's existing records retention schedules.

Covered Components must:

i. Implement procedures, using a disposal destruction method to be approved by Pitt IT Security, to address the final disposition of the PHI, including EPHI, and/or the hardware or electronic media on which it is stored
ii. Document the disposal of PHI using a form, indicating the date and method of destruction and the person(s) responsible, as well as the dates of the records that were destroyed and a statement that the records were destroyed in the normal course of business.

V. Training

All University members within a Covered Component must complete annual HIPAA training and receive additional annual training regarding HIPAA procedures within their component. PHI Workforce members must also complete annual training. To ensure compliance with the HIPAA training requirement, the annual HIPAA training and retraining for Covered Components will include, but not be limited to, privacy and security training related to PHI.

Covered Components, Business Associates, and PHI Workforce Members must:

i. Complete annual required online training required for their school/department/unit. The Office of Compliance, Investigations, and Ethics will implement and oversee these trainings. These trainings may include supplemental updates when there is a substantial change in relevant privacy policies and/or regulations.
ii. Ensure that employees, students, and volunteers receive annual training to assure their understanding of school/department/unit-specific privacy policies and procedures related to HIPAA and/or protecting PHI.
iii. Each new member of the workforce or new volunteer must be trained on school/department/unit-specific privacy policies and procedures related to HIPAA and/or protecting PHI as part of their general employment orientation.
iv. Covered Components and schools/departments/units with PHI Workforce Members should notify the Office of Compliance, Investigations, and Ethics when new employees are hired to ensure access to the required trainings.

VI. Audits and Annual Reports

a. The University Privacy Officer shall:

- **i.** Review requests for sale of PHI
- **ii.** Administer the complaint process in compliance with HIPAA
- **iii.** Maintain a list of Covered Components
- **iv.** Collect and review annual security and compliance reviews from Covered Components
- **v.** Review any reports of a security breaches and unauthorized disclosures involving PHI and perform a full breach analysis.
    - A full breach analysis considers all of the following: the nature of the PHI in question, the actors involved in the breach, the evidence of access or disclosure, and the mitigation of risk.
- **vi.** Follow the Cyber Incident Response Plan for all identified breaches with the support of the Office of Compliance, Investigations & Ethics, the Director of Enterprise Risk, the Office of Internal Audit, Pitt IT Security, the Office of University Counsel, and others.

b. The Office of Compliance, Investigations and Ethics shall:

- **i.** Maintain and annually review the list of component-specific HIPAA Privacy Officers
- **ii.** Maintain and annually review the list of component-specific HIPAA Security Officials
- **iii.** Annually collect and review records of disclosures made from Covered Components
- **iv.** Maintain a list of HIPAA Business Associates and executed Business Associate Agreements
- **v.** Maintain forms, documents, and templates for use by Covered Components
- **vi.** Collect reports of requests for amendments to PHI
- **vii.** Maintain a list of PHI Workforce Members who require annual HIPAA training
- **viii.** Audit Covered Components and PHI Workforce Members HIPAA training completion

c. The University HIPAA Security Official shall:

- **i.** Collaborate with the CISO and Pitt IT to ensure that safeguards protecting EPHI are in place
- **ii.** Collect responses and remediation recommendations to non-compliance from Component Security Officials
- **iii.** Collect and review annual security and compliance reviews from Covered Components

VII. Complaints

Complaints arising in regards to the University's HIPAA policy may be submitted by email to the University Privacy Officer (compliance@pitt.edu), or by submitting a concern to the Pitt Concern Connection, or directed to the Secretary of the U.S. Department of Health and Human Services if they believe their rights have been violated.