HIPAA Compliance Program: Guidance for Component Privacy Officers

I. Purpose

This document provides detailed guidance to Component-specific HIPAA Privacy Officers ("Component Privacy Officers") required to act in accordance with University Health Insurance Portability and Accountability Act (HIPAA) Policy and HIPAA's Privacy Rule. These individuals are appointed by Covered Components. This document is designed to be used in conjunction with the accompanying HIPAA Compliance Program.

II. Covered Components

A HIPAA Covered Component is an area of the University that serves as a health care provider, health plan, or health care clearinghouse that transmits health information electronically in connection with financial or administrative activities. These activities 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
- University Dental Health Services

Covered Components of the University and their University Members must comply with privacy and security practices in the use, storage, and disclosure of Personal Health Information (PHI) and Electronic Personal Health Information (ePHI) as required by HIPAA. Procedures may vary by Covered Components, but all Component Privacy Officers are expected to adhere to the standards outlined in this document.

III. Responsibilities of Component-specific HIPAA Privacy Officers

The Component Privacy Officer oversees all ongoing activities related to the implementation of, maintenance of, and adherence to the university's policies and procedures related to HIPAA within their assigned covered component.

HIPAA Privacy Officer responsibilities include:

1. Ensure full coordination and cooperation with University Policy and Procedure
2. Ensure that the Covered Component Requirements (below) are met, utilizing appropriate forms, notices, and materials
3. Ensure adherence to correct procedures for tracking access to PHI and for allowing individuals to review and report on such activities
4. Ensure reporting protocols and schedules are followed as established
5. Perform periodic privacy risk assessments and conduct compliance monitoring activities in coordination with the CIE Office

6. Oversee, direct, deliver, or ensure delivery of initial and ongoing HIPAA and privacy training for component employees, Business Associates and other appropriate third parties
7. Participate in the development and implementation of Business Associate Agreements and monitor compliance with these agreements
8. Serve as Covered Component's Case Manager in Pitt Concern Connection for all HIPAA-related concerns associated with the Covered Component
9. Cooperate in any compliance reviews or investigations

IV. Covered Component Requirements

Covered components have the following compliance obligations under HIPAA.

a. Notices
    i. Provide Notice of University Privacy Practices available by request, to anyone and publish the notice on the component's website
    ii. *(For components that provide treatment)* provide the 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
b. Disclosure Accounting
    i. Track disclosures of PHI
        i. *PHI Use and Disclosure Tracking Form*
        ii. To be submitted to the CIE Office on an annual basis (compliance@pitt.edu)
    ii. Establish component-specific procedures for responding to Disclosure Accounting Requests
        i. *Individual Request for Disclosure Accounting Form*
    iii. Adhere to procedures for responding to Disclosure Accounting Request for Business Associates
        i. A requestor may contact a Business Associate directly to request an accounting of the Business Associate's uses and disclosures of their EPHI. A list of all HIPAA Business Associates is available upon request from the Office of Compliance, Investigations and Ethics (compliance@pitt.edu).
c. Use and Disclosure of PHI
    i. Fundraising
        i. Ensure that proper permissions and documentation have been obtained from the University Privacy Officer prior to engaging in the sale of PHI
    ii. Marketing
        i. Contact the University's Privacy Officer to obtain a valid authorization form for the use of PHI for marketing purposes

iii. Sale
    i. Contact the University's Privacy Officer to obtain a valid authorization form to sell or receive payment in exchange for disclosing PHI

d. Amendments to PHI
    i. Respond to amendment requests within 60 days of receiving the request
        i. One 30-day extension is permitted if the Covered Component provides the requestor with a written statement of the reasons for the delay and the date by which the Covered Component will complete the request.
    ii. Report all requests for amendments to PHI to the CIE Office (compliance@pitt.edu)
    iii. Establish component-specific procedures for approval and denial of amendment requests using forms and templates available from the CIE Office
        i. *Individual Amendment to PHI Request Form*
        ii. *Covered Component PHI Amendment Approval Letter Template*
        iii. *Covered Component PHI Amendment Full Denial Letter Template*
        iv. *Covered Component PHI Amendment Partial Denial Letter Template*

e. Visitors
    i. Ensure that visitors are sponsored by an individual from a University management position
        i. Ensure that visitors are accompanied by a University staff member at all times during the visit
        ii. If a visitor is expected to come into contact with patients or PHI during the visit, ensure that the visitor signs a confidentiality agreement prior to beginning visit activities
            a. *Visitor Confidentiality Agreement*
        iii. If a visitor comes into direct contact with a patient, the accompanying University staff member shall get approval from the patient prior to the visitor having contact with the patient

f. Training
    i. Ensure that component employees receive and complete annual training to assure their understanding of HIPAA privacy policies and procedures
        i. Each new member of the component workforce must be trained on HIPAA privacy policies and procedures as part of their general employment orientation
            a. Ensure that the HIPAA training requirement appears on job requisition forms for open positions

b. Notify the Office of Compliance, Investigations, and Ethics when new employees are hired to ensure access to the required trainings.

g. Complaints
   i. Assist individuals wishing to make a complaint in regard to the University's HIPAA policy.
      i. Complaints may be submitted via email to the University Privacy Officer, via the Pitt Concern Connection, or directed to the Secretary of the U.S. Department of Health and Human Services.
         a. *HIPAA Privacy Complaint Form*

V. Support

University Privacy Officer

The University Privacy Officer is tasked with ensuring that the University's collection, use, and disclosure of personal information complies with federal regulations, including HIPAA.
University Privacy Officer responsibilities include:

- Oversee all ongoing activities related to the development of, implementation of, and adherence to the University's HIPAA Compliance Program
- Maintain a list of Covered Components and PHI Workforce Members
- Collect and review annual security and compliance reviews from Covered Components
- Administration of the complaint process in compliance with HIPAA
- Authorize and ensure proper permissions are in place prior to the Sale of PHI
- Work collaboratively with Component Privacy Officers, Component Security Officials, and the University HIPAA Security Officer to ensure HIPAA compliance

VI. Reporting Violations Regarding HIPAA Non-compliance

Violations regarding the HIPAA Privacy Rule should be reported immediately to the University Privacy Officer. The University Privacy Officer may consult with the Component Privacy Officer Official and the University's HIPAA Security Official, Office of General Counsel, and Human Resources to determine the extent of the violation and the appropriate course of action.

VII. Disciplinary Action

Violations of this guidance and failure to comply with HIPAA Privacy Rule may result in disciplinary action in accordance with University Policies.