HIPAA Compliance Program: Guidance for Component Security Officials

I. Purpose

This document provides detailed guidance to Component-specific HIPAA Security Officials ("Component Security Officials") required to act in accordance with University Health Insurance Portability and Accountability Act (HIPAA) Policy (CS 30) and HIPAA's Security Rule. These individuals are nominated by Covered Components and approved/confirmed by the University HIPAA Security Officer. They serve as security officials in designated University Covered Components. This document is designed to be used in conjunction with the 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 healthcare 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 Security Officials are expected to adhere to the standards outlined in this document.

III. Responsibilities of Component-specific HIPAA Security Officials

The 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.

Component Security Official responsibilities include:

1. Understanding, implementing, managing, and enforcing information security directives as outlined in the University HIPAA Policy and Procedure,

A. Security directives shall comply with the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164.)
B. Health and Human Services (HHS) guidance for implementing and complying with the HIPAA Security Rule's administrative, technical, and physical controls can be found at:
    I. https://www.hhs.gov/hipaa/for-professionals/security/index.html
    II. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

2. Assisting with annual Covered Component HIPAA Security Rule risk and controls assessment
3. Assisting with developing HIPAA Security Rule compliance remediation plans, including assigning and procuring resources
4. Reporting and assisting with HIPAA Security Rule violation investigations

IV. Support

University HIPAA Security Officer

Pitt IT, the University's Chief Information Security Officer (CISO), and Covered Components share responsibility for the University's compliance with the HIPAA Security rule. The CISO has delegated authority under Policy CS 30 to the University HIPAA Security Officer, who has the following responsibilities:

Responsibilities of the University HIPAA Security Officer include:

1. Overseeing the University's Component Security Officials regarding HIPAA Security Rule implementation and compliance
2. Providing HIPAA Security Rule guidance to the Component Security Officials
3. Performing annual Covered Component HIPAA Security Rule risk and controls assessments utilizing the Health and Human Services Audit Protocol (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html)
4. Overseeing investigations of reported violations of the HIPAA Security Rule
5. Reviewing this process annually with Component Security Officials

V. Reporting Violations Regarding HIPAA Non-compliance

Violations regarding the HIPAA Security Rule should be reported immediately to the University's HIPAA Security Officer via the 24/7 IT Help Desk at 412-624-HELP (4357). The University's HIPAA Security Officer may consult with the Component Security Official and the University's Privacy Officer, Office of

General Counsel, and Human Resources to determine the extent of the violation and the appropriate course of action.

VI. Disciplinary Action

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