UPMC | SCHOOLS OF NURSING

UPMC SCHOOLS OF NURSING
POLICY AND PROCEDURE

SUBJECT: Student Information Security **INDEX TITLE: Administrative**
DATE: September 18, 2024

I. POLICY:

It is the policy of the UPMC Schools of Nursing (SON) to implement and maintain a comprehensive Information Security program that contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of our institution.

II. PURPOSE:

The purpose of this policy is to address UPMC SON campus wide strategies and responsibilities for protecting the security, confidentiality and integrity of student information.

III. SCOPE:

This policy applies to each school within the UPMC SON.

IV. REFERENCES AND GUIDELINES:

The Safeguards Rule (16 CFR Part 314) requires financial institutions under the Federal Trade Commission jurisdiction to have measures in place to keep student financial information secure. In addition to developing safeguards, UPMC Schools of Nursing (UPMC SON) is responsible for taking steps to ensure that affiliates and service providers safeguard customer information in their care. The Gramm-Leach-Bliley Act (GLBA), requires the UPMC Schools of Nursing to develop, implement and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of student financial information The UPMC Schools of Nursing maintain a Student Information System to house demographic, admission, financial, and educational student documentation.

The UPMC SON has developed, implemented, and maintains a comprehensive information security program consisting of eight fundamentals that address administrative, technical, and physical safeguards that are appropriate to the size and complexity of our school by:

1. Appointing a qualified designee to facilitate, enforce and oversee the UPMC SON Student Information Security Program
2. Assessing and identifying internal and external risks to the security, confidentiality and integrity of student financial information
3. Designing and implementing safeguards to control risk
4. Monitoring, testing and assessing the vulnerability of information systems
5. Training and educating users on Student Information Security

6. Overseeing service providers
7. Establishing an incident response plan
8. Reporting the Information Security Program outcomes to leadership

The UPMC SON appoints the Manager of Compliance and Reporting as the coordinator of the information security program. The Manager of Compliance and Reporting in conjunction with the UPMC SON Educational Technology Specialist will implement and maintain the security program for all UPMC SON campuses and complete an annual review to ensure effectiveness.

The UPMC SON Manager of Compliance and Reporting will oversee the Student Information System (SIS) Steering Committee which consists of key members from cross-functional departments to provide a diverse range of experience in the areas of auditing, compliance, controls, IT management, IT security and risk assessment. The SIS Steering Committee is responsible for identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information.

The SIS Steering Committee will review the information security program on a quarterly basis to evaluate and, if necessary, adjust the UPMC SON Information Security program considering the results of the testing and monitoring outlined in final assessment, review and/or audit reports.

Reviewed/Revised: 09/18/2024
Originated: 03/05/19
Effective Date: 09/18/2024