# Augusta University / AU Health System

Information Security Training Policy

Policy Owner: Chief Privacy Officer

## POLICY STATEMENT

This policy applies to all employees and staff of Augusta University (AU), AU Health System Inc. (AUHS), AU Medical Center Inc. (AUMC), AU Medical Associates Inc. (AUMA), Roosevelt Warm Springs Rehabilitation and Specialty Hospitals, Inc. (RWSH), and all related or affiliated University or Health System entities or clinical sites, hereinafter referred to collectively as "AU Enterprise". This policy applies to all duties of AU Enterprise employees and staff performed within the scope of their employment at any site of the AU Enterprise.

AU Enterprise is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), and/or other sensitive information (SEI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to SEI, PHI, or ePHI.

## AFFECTED STAKEHOLDERS

*Indicate all entities and persons within the Enterprise that are affected by this policy:*

☒ AU Enterprise staff, including permanent, temporary, and part-time
☒ House staff, Residents, & Clinical Fellows
☒ Independent and Employed credentialed providers and Medical Staff
☒ Vendors/Contractors
☒ Researchers, students
☒ Any other individual with a relationship to AU or AU Health System that may create, use, disclose or access sensitive information

## DEFINITIONS

Protected Health Information (PHI): PHI as defined in the Health Insurance Portability and Accountability Act of 1996 privacy regulations, ("HIPAA"), as amended.

Sensitive Electronic Information: any information relating to identified or identifiable individual or entity that is confidential, proprietary, or sensitive to such individual or entity and may cause harm to such individual or entity if accessed, used, or disclosed by unauthorized persons, or lost, either internal or external to AU or AU Health. This includes, but is not limited to Confidential Information, Protected Health Information, Personally Identifiable Information, Payment Card Industry (PCI) data, undisclosed financial statements, audit reports, and other information subject to any valid exception to the Georgia Open Records Law.

## RESPONSIBILITIES

- Responsibility - It is the responsibility of the Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) to develop, implement, and manage the information security and privacy training program.

- Program Contents - The information security and privacy awareness and training program content will include a basic understanding of information security and privacy and the actions required to maintain security and to respond to suspected security incidents. The information security and privacy program should include topics such as the following:

    - The HIPAA Security Rule (*§ 164.308(a)(5)*):
        - Definition of SEI
        - Definition of PHI and e-PHI
        - Security Reminders
        - Protection from Malicious Software
        - Log-in Monitoring
        - Password Management
        - Workstation Security
        - Usage and Login Monitoring
        - Access Controls
        - Insider Threats
        - Incident and Breach handling procedures for employees
        - Names and contact information for the CISO, CPO, and Compliance Reporting Line.
        - AU Security and Privacy Policy and Procedure.
        - Expectations of compliance and AU Sanctions Policy for noncompliance.

- Program Compliance
    - Basic security and privacy training will be held upon hire and annually thereafter for all workforce members who come into contact with PHI or SEI.
    - Advanced security and privacy training for IT staff will be held upon hire and annually thereafter.
    - This content must be appropriate for the workforce members' knowledge, role, and responsibilities.
    - The Security Awareness and Training shall be reviewed at least annually or within a reasonable after there are significant changes to the HIPAA .
    - When information is obtained that could improve the information security and privacy training program or any shortcomings of the program are discovered, the program should be updated.
    - The information security and privacy training program will be protected, controlled, and retained in accordance with federal, state, and organizational requirements.
    - Remedial training will be required of workforce members as necessary response to a privacy or information security incident.

- Each workforce member's completed training is electronically recorded within the learning management system (LMS). Training transcripts may be printed after the courses are completed. Training content and learning reports must be retained for six years from the date of their creation or the date when it was last in effect, whichever is later.
- It is the workforce member's duty to complete all training assignments.
    - The Office of Compliance is responsible for ensuring training compliance with the staff under their supervision.
    - The Office of Compliance in collaboration with Information Security Division, and Human Resources Workforce Development oversees the auditing and monitoring of privacy, confidentiality and information security workforce training.
- Failure to complete assigned information security and privacy training will result in the workforce member's loss of access to PHI until the assignment is completed or may result in other disciplinary action.

## REFERENCES, SUPPORTING DOCUMENTS, AND TOOLS

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy and Security regulations
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended (including the Breach Notification Rule.

## RELATED POLICIES

N/A

## APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 2/22/2019

President, Augusta University and CEO, AU Health System
Date: 2/27/2019