Augusta University / AU Health System

Electronic Information Security Policy

Policy Manager: Chief Information Security 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.

The information security program provides a sustainable consistent approach to information safeguards that can be replicated across electronic files, systems and transactions. This information is contained in many forms in electronic records.

The AU Enterprise information security program provides the framework, methodology, and practices to ensure that all sensitive information (SEI), including all electronic protected health information (ePHI), is appropriately secure throughout the AU Enterprise system, irrespective of the medium used.

It is the policy of AU Enterprise to ensure that all SEI and ePHI are protected whether that information is at rest or in motion. The Information Security Program will use all reasonable control measures to protect information against unauthorized access and use, maintain the integrity of all information, ensure that access to information is timely and appropriate, and will ensure compliance with all applicable state and federal laws and appropriate standards such as; the Health Insurance Portability and Accountability Act ("HIPAA"), Payment Card Industry (PCI), and the University System of Georgia, Board of Regents Policy 10.4, Cybersecurity.

To ensure the protection of SEI and ePHI it is the policy of Augusta Enterprise to prohibit the practice of sending, sharing, or disclosing in any way SEI or ePHI from any AU Enterprise account or system without the appropriate protective measures in place.

Office of Legal Affairs Use Only
Policy Sponsor: VP of Information Technology
Next Review: 2/2020

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

Device: any media, material, or type of equipment that records, stores, transmits, distributes, or uses electronic information. This includes, but is not limited to, computers (hard drives), any removable/transferrable digital memory, disks, memory cards, cloud storage, internet, extranet or any other device which involves the access, storage, or creation of sensitive information.

Encryption: Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.

PCI DSS - The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

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

Sensitive 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 Exception 25 of the Georgia Sunshine Act

PROCESS & PROCEDURES

I. Information Security Program Roles and Responsibilities:

- Chief Information Security Officer (CISO);
    - Provides solutions, guidance, and expertise in IT security.
    - Facilitates effective implementation of the AU Information Security Program, by:

        - Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;
        - Collecting data relative to the state of IT security across the AU environment collectively and communicating that state to the Compliance Team quarterly,
        - Consult with university leaders and staff to ensure an effective balance between the information security program and business needs,
        - Maintains awareness of the security status of all sensitive IT systems,
        - Develops, implements, and maintains an information security awareness and training program for all users,
        - Mitigate and report all known or suspected security incidents and ensure appropriate actions are taken to prevent recurrence.
        - Ensure a comprehensive system and data classification process is developed, implemented, and maintained.
        - Develops, implements, and maintains a comprehensive IT risk management and assessment.

- Users will;
    - Be knowledgeable of all pertinent information security policies and comply with information security program requirements.
    - Report security incidents and/or breaches, actual or suspected, to the CISO.
    - Taking reasonable and prudent steps in compliance with enterprise AU policies and procedures and best practices to protect the security of IT systems and data to which they have access.
    - Ensure that no SEI or ePHI is sent, shared, or disclosed in any way from any Augusta University, AU Health System, Inc., AU Medical Center, Inc. or AU Medical Associates, Inc. account or system without the appropriate protective measures in place.

II. Information Security Program Components

- Systems Risk Management
    - Systems risk management addresses protecting information and IT systems commensurate with sensitivity and risk, including system availability.

- IT Contingency Planning
    - Contingency planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and information that support essential business functions if an event occurs that renders the IT systems and information unavailable. Contingency Planning includes Continuity of Operations Planning, Disaster Recovery Planning, and IT System Backup and Restoration.

- IT Systems Security
    - Systems Security defines the steps necessary to provide adequate and effective protection for IT systems such as; systems security plans, hardening, malicious code protection, and systems development security.

- Data Protection
  - Data protection provides safeguards for the processing and storing of data. Data Protection includes requirements in the areas of media protection and encryption.

- Threat Management
  - Threat management addresses the protection of systems and information by preparing for and responding to information security incidents. This includes threat detection, incident handling, and security monitoring and logging.

- Asset Management
  - Asset management includes IT asset control, software license management, and configuration management and change control.

REFERENCES, SUPPORTING DOCUMENTS, AND TOOLS

- Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security regulations
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended

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