Augusta University / AU Health System

Encryption 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.

This policy addresses the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations (as well as changes made through the Health Information Technology of Economic and Clinical Health Act (HITECH)), and other applicable federal, state, or local laws and regulations that may relate to the protection and security of SEI through the use of encryption technologies to render this information unreadable while at rest and in motion.

Augusta Enterprise shall encrypt ePHI stored at rest to meet the implementation specification requirements in the HIPAA *Access Control* standard.

Augusta Enterprise shall encrypt ePHI that traverses the Internet to meet the implementation specification requirements in the HIPAA *Transmission Security* standard.

Business systems managers of any system(s) within or utilized by the Augusta Enterprise that cannot be encrypted due to technical limitations shall submit a waiver to the Chief Information Security Officer (CISO). The CISO may grant waivers to this policy providing compensating controls are documented.

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

Cloud: a computing infrastructure of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

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. Mobile Devices are a subset of devices that reside outside of a traditional data center and can be removed or transported by one person, e.g., laptops, tablets, smartphones, memory sticks, removable hard drives, biomedical equipment

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.

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

Safe Harbor: The process of rendering unsecured protected health information unreadable held in electronic media, protecting the encryption key, and proving the above after the media is lost or stolen.

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.

AU Enterprise Workforce: All persons working in any entity of the AU Enterprise who are full-time or part-time employees, trainees, vendors, contractors, or any other individuals who may create, use, disclose, access, or transmit any sensitive information.

Unsecured protected health information: protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary (of HHS) in the guidance issued under section 13402(h)(2) of Public Law 111-5. This guidance specifies that only encryption and destruction, consistent with National Institute of Standards and Technology (NIST) guidelines, renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that notification is not required in the event of a breach of such information.

STANDARD

Device encryption must address the following as defined by HIPAA and NIST:

- Proof that the data is sufficiently scrambled in a way that a third party could not possibly extract data from a lost or stolen hard drive or device,
- The key used to scramble the data must be strong enough to prevent guessing, even using brute force programs, and
- Controls must be in place to prove compliance with this standard if a device is missing.

Device encryption should address the following technical requirements as defined by HIPAA and NIST:

- Make a reasonable effort to ensure that all devices are properly encrypted before accessing, creating, or storing SI,
- Not store ePHI on unencrypted devices, and
- Promptly report lost, stolen, or compromised devices to law enforcement or any member of the Compliance Team.

RESPONSIBILITIES

I. The CISO shall make a reasonable effort to ensure:

- That all devices that may access, store, or create SI are inventoried and encrypted using methods that comply with this standard.
- That data is properly encrypted at rest and while in motion within reasonable industry standards or data security is otherwise addressed and documented.
- That the AU Enterprise workforce is provided with the adequate tools and equipment to properly access, store, create, and transmit sensitive Information.

II. The CISO shall:

- Establish specific encryption standards to support encryption in a manner consistent with applicable regulatory standards and provide adequate protections for SI and to comply with HIPAA, HITECH, and other applicable federal, state, or local laws and regulations that may relate to:
    - The protection and security of all sensitive information,
    - The protection and security of systems that accesses sensitive information, and
    - The protection and security of the methods used to access both systems and sensitive information within them.

- That all waiver requests are reviewed to determine the level of risk to the organizations prior to approval.

III. Sanctions:

- Failure to comply with this policy will result in disciplinary actions, up to and including termination.

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
- NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices
- NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- NIST Special Publication 800-77 Guide to IPsec VPNs
- NIST Special Publication 800-113 Guide to SSL VPNs
- And other FIPS 140-2 validated processes
- Payment Card Industry (PCI) PCI Security Standards Council

RELATED POLICIES

Electronic Access Control Policy

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