Augusta University/AU Health System

Electronic Data Retention Policy for Protected Health Information

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

This policy applies to all employees of Augusta University when they are working in a AU Health System clinical setting, and applies to all employees of the AU Health System, Inc. to include: AU Medical Center, Inc. (AUMC), AU Medical Associates, Inc. (AUMA), and Roosevelt Warm Springs Rehabilitation and Specialty Hospitals, Inc. (RWSH) performing duties within the scope of their employment at any site.

AU Enterprise is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), and/or other sensitive electronic 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:

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

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.

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 applicable provisions of the Georgia Open Records Act O.C.G.A. § 50-18-70 et seq.

PROCESS & PROCEDURES

I. Retention Schedule Guidelines:

- The listed retention period for each record is the minimum period of time that a record must be maintained to meet legal and/or fiscal directives.
- If no retention criterion exists for a particular record, the retention period is equal to the Georgia statute of limitations for legal claims, plus one year for that record type.
- Records designated as permanent must be maintained in an archive as a part of the historical record for long term preservation. If no record archive is available, the records must be stored as a 'record copy' and maintained in the original format.

II. Retention Archives:

- Record archives must employ appropriate encryption methodologies to protect SEI and ePHI from unauthorized access while the record is retained.
- Information subject to the retention schedules identified herein should be stored in an appropriate record archive and not on individual devices.
- Information contained within the body or in an attachment of an email are subject to the retention schedules identified herein. Information or attachments that meet retention criteria must be removed from the email system and stored in an identified archive location.

III. Record Disposal:

- Records that have exceed the retention period must be disposed of or archived in accordance with the data disposal requirements for that record type.

IV. 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
- USG Records Management and Archives
- USG Records Retention Schedules

RELATED POLICIES

N/A

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 4/3/2019

President, Augusta University and CEO, AU Health System
Date: 4/19/2019