Augusta University/AU Health System

AU Enterprise Electronic Data Access Control Policy

Policy Manager: Chief Technology Officer

POLICY STATEMENT

This policy applies to all employees and staff of the legal entities of Augusta University (AU) and the AU Health System to include: AU Health System, Inc. (AUHS), 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:

☒ AU staff, including permanent, temporary, and part-time
☒ AUHS, AUMC, AUMA, RWHS 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

Departmental Security Authority: Roles that include requesting access and permissions for various AU Enterprise clinical and administrative systems, assisting in information security awareness training and cooperating with the Chief Compliance Officer, Chief Privacy Officer, Chief Information Security Officer, Human Resources, and Public Safety with incident investigations.

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

Remote Access: Using any device, regardless of ownership, to access AU or AU Health information or information systems from outside the enterprise network. Examples would include: virtual private network (VPN), email access offsite, Citrix web access offsite, etc.

Split-tunneling: The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. This method of network access enables the user to access remote devices, such as a networked printer, at the same time as accessing the public network.

PROCESS & PROCEDURES

I. Access Control Methods

- The following methods are employed by AU, AUHS, AUMC, AUMA, and RWSH to ensure the confidentiality, integrity and availability of the information and resources available.

    - User access controls:
        - All users are assigned unique usernames and passwords/phrases for all systems.
        - Background checks, appropriate for each position and its level of access, are completed for all potential users before access is granted.
        - All access to information systems will be based on the workforce members’ role within the organization. Workforce members will not be granted access to systems or information that they do not have a legitimate business need to access.
        - All users will lock, log off, or lock out of all workstations or systems when they are not actively being used.
        - Accounts will not be shared among users; no user will allow anyone else to use a workstation or system under their unique user ID and password.
        - AU vendors and contractors must have a completed BAA, non-disclosure agreement, and confidentiality agreement on file.

- IT Access Controls:
  - Credentials are securely managed and not disseminated through unsecure mediums.
  - All access control devices (tokens, FOBS, access cards, etc.) are controlled and tracked through the Information Security Office.
  - Identity verification methods are employed before any modifications to an account are made.
  - All sessions will terminate after 15 minutes of inactivity; both internal connections and remote.

II. Access Termination

- Terminations will be processed immediately, all accounts and access of a terminated AU or AUHS workforce member, vendor, or contractor will be terminated;
-

1. Within 24 hours for any workforce member, vendor, or contractor that does not have elevated access or account privileges,
2. Immediately for all accounts that have elevated access or account privileges, and
3. Immediately for all involuntary terminations or those not following normal resignation processes.

III. Remote Access

- AU and AUHS workforce, vendors, contractors, and any other users granted remote access to the AU Enterprise network, information, or other electronic resources must:
  - AU and AUHS vendors and contractors must have a completed BAA, non-disclosure agreement, and confidentiality agreement on file.
  - Ensure that their remote access credentials, software, and configuration are protected.
  - All remote access connections will require the use of multi-factor authentication.
  - Remote access to ePHI is only granted to authorized users based on their role within the AU Enterprise organization.
  - All remote access connections must utilize only approved, encrypted connection methods for secure data transmission.
  - At no time shall any user share or provide their login or password to anyone.
  - No workstation that is remotely connected to the AU Enterprise network will connect or be connected to any other network at the same time.
  - Reconfiguration of equipment for the purpose of split-tunneling or dual homing is not permitted.
  - Workstations with remote access privileges to the AU Enterprise network will not be shared.
  - All devices that connect to the AU Enterprise network via remote access will have up-to-date anti-virus software and current operating system and software patches.

- Remote Access Requests
  - Contractors, vendors, or workforce members requiring remote access will submit the request to the appropriate Departmental Security Authority (SA) for processing.
  - All requests for remote access will be reviewed for;
    - Accuracy,

        - Technical considerations,
        - Security considerations, and
        - Appropriateness of the request.
    - All remote access requests require the approval of the CIO and CISO or their designees.

- Remote Access Termination
    - Remote access privileges can be revoked by the CIO or CISO or their designees at any time deemed necessary.
    - Remote access privileges will be terminated immediately upon the termination of a workforce member.
    - Remote access privileges will be terminated immediately upon the termination of a contractor, vendor, or other non-AU workforce members.

IV. Notice of Incident or Breach

- In the event that an incident or data breach (i.e. information security incident) occurs during the course of remote access to confidential/regulated data, the workforce member and/or the Business Associate is required to immediately notify the Information Security Office at 706-721-SAFE (8233) or the Compliance Hotline at 1-800-576-6623. Both are available 24 hours/7 days a week/365 days a year.

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

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