Augusta University
Policy Library

Electronic Data Retention Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT
This policy applies to all employees and staff of Augusta University (AU), hereinafter referred to as "AU". This policy applies to all AU employees and staff performing duties within the scope of their employment at any site. AU is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), and/or other Sensitive Information (SI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to PHI, ePHI, PII, Payment Card Industry (PCI) data, or SEI. AU is committed to protecting electronic Protected Health Information (ePHI), and/or other SI by implementing physical and technical security standards within facilities and within areas of a facility that contain or provide access to sensitive information that must be protected by the institution.

This policy is in accordance with requirements of the University System of Georgia (USG) IT Handbook v 2.9.7.1

This policy addresses the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations, and other applicable federal, state, or local laws and regulations that may relate to the protection and security of information.

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

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☒ Other: Any other individual with a relationship to AU that may create, use, disclose, or access SEI or protected health information in a clinical or AU setting.

PROCESS & PROCEDURES
Users will adhere to the following regarding retention schedule guidelines, retention archives, record disposal, and compliance:

a. Retention Schedule Guidelines:

1) The listed retention period for each record is the minimum period that a record must be maintained to meet legal and/or fiscal directives.
2) If no retention criterion exists for a record, the retention period is equal to the Georgia statute of limitations for legal claims, plus one year for that record type.

3) 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.

b. Retention Archives:

1) Record archives must employ appropriate encryption methodologies to protect enterprise SI and ePHI from unauthorized access while the record is retained.
2) Information subject to the retention schedules identified herein will be stored in an appropriate record archive and not on individual devices or within unapproved applications.
3) 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.
4) The following file storage areas are available:

i. SHARE – Every department has a folder in which its members can share and collaborate on their data files. Program files are not permitted in this storage area.
ii. BOX – Box is a secure file sharing and collaboration system that is delivered through a strategic partnership between AU and Box. Special procedures related to Box storage:

1. Confidential and regulated data (Student records, PHI, etc.) may be stored within Box if there is legitimate business need and with an approved request from IT.
2. Enterprise-owned devices must be encrypted if they utilize the data synchronization capabilities of Box to store confidential/regulated data. Confidential and regulated data shall be restricted to those who have a legitimate business need to know the information using access controls available through Box including username and passwords.
3. Links that do not require authentication will never be used to store confidential or regulated data.
4. Only enterprise owned devices shall have the synchronization client installed. Clients will not be installed on personally owned devices.
5. Anyone who wishes to use a third-party cloud application that interfaces with Box must receive prior approval through the IT procurement process.
6. Box storage will be used for legitimate AU business purposes only.

c. Record Disposal: Records that exceed the retention period must be disposed of or archived in accordance with the data disposal requirements for that record type.

d. Compliance: Failure to comply with this policy will result in disciplinary actions, up to and including termination as stated in AU Personnel Policies and Human Resource Work Rules.

REFERENCES & SUPPORTING DOCUMENTS
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 IT Handbook v2.7.9.1
Georgia Open Records Act - Official Code of Georgia Annotated (O.C.G.A.) § 50-18-92(a) USG
Records Management and Archives
USG Records Retention Schedules

RELATED POLICIES
Cybersecurity Program (Charter) Policy
Data Management and Classification Policy
Electronic Data Storage Backup Policy
Encryption Policy

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 11/28/2023

President, Augusta University Date: 11/29/2023