PURPOSE

To ensure correct interpretation and Integrity of data extracted from, transmitted, or stored in the University of Arkansas for Medical Sciences ("UAMS") enterprise and departmental systems.

SCOPE

UAMS Workforce with access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee and student information, information concerning UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential Information shall include Protected Health Information. Confidential Information includes information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

Electronic Protected Health Information (ePHI) means individually identifiable health information that is:

- Transmitted/Received by Electronic media
- Maintained in Electronic media

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

Integrity means that data or information have not been altered or destroyed in an unauthorized manner.

Data Custodians are individuals who have the primary responsibility for the accuracy, privacy, and security of the UAMS Data under their purview, providing specific data management and maintenance responsibilities.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future

payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer and health information regarding a person who has been deceased for more than 50 years.

UAMS Workforce means for the purpose of this Policy, physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

Other terms or definitions referenced in this policy are available on the UAMS HIPAA Office website at hipaa.uams.edu.

POLICY

UAMS will implement appropriate data Authentication measures to protect the Integrity of Confidential Information, including ePHI, and to protect against improper and unauthorized alteration or destruction. Data Authentication measures will include formal and documented electronic processes to validate data Integrity and to verify that the data sent is identical to the data received. Encryption methods must be utilized for all sytems such as laptops, workstations, and mobile devices outside the perimeter of enterprise data centers that manage any data containing Confidential Information, including ePHI.

PROCEDURES

A. Enterprise Data Integrity

1. Commercial products will be utilized as the standard basis for the collection, manipulation, and storage of UAMS data. Programming changes made to these products must be thoroughly tested prior to moving into production.
2. A formal change control process must be used when making changes to the operating system or application layer on all UAMS systems.
3. All systems must be protected at a minimum by user IDs and passwords and reside in a physically secure location. Multi-factor authentication (MFA) will be utilized for remote access and when appropriate for systems containing Confidential Information.
4. All systems should be consistent in availability, performance, and efficiency providing access to data that compliments necessary workflows.
5. All systems must be configured to follow guidelines outlined in the UAMS Disaster Recovery policy.
6. All systems, computers, devices, software, and network equipment must meet cybersecurity and regulatory requirements, including proper patching and operating system levels.
7. Users must be trained in the proper use of the system and provided contacts for resolving problems.
8. All systems must be well maintained with all necessary updates and proper upgrades.
9. Data Custodians must ensure the data values for the elements within their charge are correct and make timely, documented corrective actions when necessary.

10. Data Loss Prevention processes will be utilized to protect UAMS information based upon data classification. See data classification processes here: UAMS Cybersecurity Procedures ver1.0.docx (sharepoint.com).

B. Data Encryption and Enterprise Data Integrity

All UAMS laptops containing or used to transmit Confidential Information including ePHI must be encrypted utilizing the UAMS enterprise whole disk Encryption. Laptops that are owned by all UAMS departments will be considered as containing Confidential Information including ePHI and required to fulfill the Encryption procedure. Any personally owned laptops utilized for UAMS business must be tagged and encrypted. UAMS data containing Confidential Information may NOT reside on an unencrypted non-UAMS laptop or desktop computer. Any UAMS desktop computer used to store or manipulate Confidential Information is also required to be encrypted as above. These procedures set the minimum standards for the enterprise Encryption of laptop computers, desktop computers, smart phones/pads, media, and other devices that hold UAMS data, or connect to the UAMS network per UAMS policies *Administrative Guide Policy 2.1.02, Mobile Device Management* and *Administrative Guide Policy 2.1.23, Safeguarding Protected Health Information*.

1. Laptops will require pre-boot user authentication where appropriate.
2. Desktop computers will not require the pre-boot authentication.
3. The entire hard drive will be encrypted using Advanced Encryption Standard (AES) 256-bit key length.
4. An audit trail will be maintained to demonstrate that a laptop was encrypted. Laptops must be brought in at least annually and joined to the UAMS network to provide this audit.
5. The Encryption process and procedures will be centrally managed by UAMS IT. This process will allow for the recovery of passwords and data in the case of emergencies.
6. Users are required to encrypt **any** UAMS data containing Confidential Information that is copied to media (thumb drives, external drives, CDs, DVDs).
7. Users are required to install the UAMS enterprise mobile device management application on their smart phone/pad in oder to access resources at UAMS.

C. **Malicious Software Preventions**

The process for malicious software prevention, detection and reporting includes, but is not limited to:

1. Establishment of Active Directory policies and placement of intrusion detection and firewalls.
2. Installation and updating of endpoint detection and response (EDR) software on all UAMS workstations, laptops, servers and other computing devices. Exceptions must be approved by IT Security.
3. The examination of electronic mail attachments and data downloads for malicious software before use on UAMS information systems.

4. An appropriate disaster recovery plan for recovering from malicious software attacks. Systems found to be infected with malicious software will be removed until the infection is removed.
5. Procedures to limit unauthorized software installation. Use of peer to peer software file sharing applications is blocked on the UAMS firewall to reduce the risk of computer worms and illegal software.
6. Home computers connecting to the UAMS network shall utilize local firewalls, and maintain updated anti-virus, anti-spyware, and operating system software. Instructions for the above can be found on the UAMS intranet at this link: https://uams.service-now.com/ess
7. UAMS Workforce members will be trained on and regularly reminded of the threat posed by malicious software, and how to identify and report possible infections.
8. UAMS Workforce members must not by-pass or disable EDR software unless appropriately authorized by UAMS IT.

SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with Administrative Guide Policy 4.4.02*, Employee Discipline* and UAMS Administrative Guide *2.1.42, HIPAA Sanctions Policy*.

REFERENCES

1) Administrative Guide Policy 2.1.35, Information Access Management
2) Administrative Guide Policy 2.1.41, Disaster Recovery

Signature:  **Date: March 11, 2024**