



NUMBER: 7.3.10

DATE: 10/20/2008

REVISION: 12/02/2008

PAGE: 1 of 2

SECTION: INFORMATION TECHNOLOGY

AREA: NETWORK SECURITY

SUBJECT: UAMS DATA ENCRYPTION

PURPOSE

The following policy and procedures establish requirements and guidelines for the installation and operation of laptop and desktop computers owned by UAMS or that contain data utilized by any representative or agent of UAMS in order to protect information technology resources and the data stored, processed, and transmitted by those resources; including any Confidential Information including ePHI.

SCOPE

UAMS Workforce.

DEFINITIONS

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.

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the 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.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, 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.

Click the following link to access any other terms or definitions referenced in this policy:

<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

POLICY

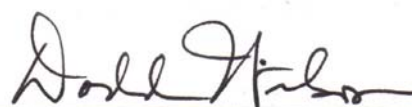
Data Encryption and Authentication:

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, media, and

other devices that hold UAMS data, or connect to the UAMS network per UAMS policies [Mobile Device Safeguards 3.1.17](#) and [Safeguarding Protected Health Information 3.1.38](#).

PROCEDURE

- Laptops will require pre-boot user authentication.
- Desktop computers will not require the pre-boot authentication.
- The entire hard drive will be encrypted using Advanced Encryption Standard (AES) 256-bit key length.
- 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.
- 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.
- Users are required to encrypt **any** UAMS data containing Confidential Information that is copied to media (thumb drives, external drives, CDs, DVDs).

SIGNATURE: 
Chancellor

Date: February 27, 2009