UAMS

UNIVERSITY OF ARKANSAS
FOR MEDICAL SCIENCES

UAMS ADMINISTRATIVE GUIDE

NUMBER: 2.1.29 **DATE: 04/01/2005**

REVISION: 11/15/2006; 02/01/2010; 3/3/2011: 01/02/2013; 05/06/2015 PAGE: 1 **of** 4

SECTION: HIPAA

AREA: HIPAA PRIVACY/SECURITY POLICIES

SUBJECT: AUTHORIZED REMOTE USE OF CONFIDENTIAL INFORMATION

PURPOSE

To establish procedures and best practices in regards to the handling and protection of UAMS data including protected health information for UAMS workforce members performing their job responsibilities from home.

SCOPE

UAMS Workforce

DEFINITIONS

UAMS Workforce means for the 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.

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.

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, 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.

Electronic Protected Health Information (ePHI) means individually identifiable health information that is transmitted by or maintained in electronic media.

Information System(s) means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, application, communications, and people.

To access any other terms or definitions referenced in this policy:
http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf

POLICY

Members of the UAMS Workforce who are authorized to work from home in an official UAMS capacity are responsible for maintaining the privacy and security of all UAMS Confidential Information, including PHI and ePHI and for following all UAMS policies and procedures related to such information.

PROCEDURE

I. Confidential Information, including PHI, may be removed from UAMS by members of the Workforce only when necessary to complete their job duties and following approval from the member's supervisor. Supervisors are responsible for ensuring that the workforce member is aware of the requirements of this policy. Supervisors are also responsible for ensuring that all Confidential Information removed from UAMS by a member of the workforce is returned or destroyed when the member returns to working on the UAMS campus or at termination.

II. The Workforce member is responsible for maintaining the privacy and security of all Confidential Information that they may be transporting, storing or accessing off-site. This includes, but is not limited to:

   A. PHI and ePHI

   B. Computers and other electronic devices that contain or access Confidential Information

   C. Confidential Working Papers

III. All Confidential Information contained in paper form must be returned to UAMS or shredded using a crosscut shredder as soon as the documents are no longer required to be maintained at home by the workforce member to complete their job. When the workforce member is no longer employed by or enrolled at UAMS, all UAMS Confidential Information must be immediately returned to UAMS, shredded or deleted.

IV. All UAMS policies are in effect whether the Workforce member is working off-site or in a UAMS facility.

A. Information Security and Password Management, Administrative Guide Policy 2.1.37

1. VPN should be utilized when possible to avoid saving data to home computers. All computers and devices storing PHI must be encrypted.

2. Any Confidential Information or ePHI sent from workstations, laptops, PDAs and other mobile devices must be encrypted.

3. When leaving a workstation or computer system unattended, the UAMS employee must lock the workstation or logout of all applications and database systems containing Confidential Information.

B. Safeguarding Protected Health Information, Administrative Guide Policy 2.1.23

1. Electronic media and printed information must be transported and stored in a secure manner. PHI or computing devices containing confidential information must never be left unattended.

2. All media containing PHI or ePHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, faxes, hard drives, diskettes, CDs or other removable electronic storage devices. Confidential information being disposed of must be shredded using a cross-cut shredder or returned to UAMS for shredding.

3. UAMS materials must be put away when not being used and kept in a locked location that is not accessible to others including children, spouse and visitors.

C. Mobile Device Safeguards, Administrative Guide Policy 2.1.02 and Enterprise Data Integrity & Encryption, Administrative Guide Policy 2.1.40

1. Anti-virus software must be installed on all home computers and mobile devices used for UAMS business, and computers and mobile devices must be password protected.

2. All home computers, mobile devices, and electronic-data storage devices including thumb drives must be encrypted in accordance with Adminstrative Guide Policy 2.1.02.

3. Employees are required to maintain updates to current operating systems (ex. Microsoft updates/patches)

D. Confidentiality Policy, Administrative Guide Policy 2.1.01

1. Passwords to computers storing Confidential Information must not be shared or made accessible to family members or others.

2. UAMS passwords must never be shared with anyone.

E. The printing of Confidential Information from home computers should be kept to a minimum and only as needed in accordance with UAMS policies.

V. Supervisors must pre-approve removal of any UAMS departmental equipment, and a UAMS Property Located Off-Campus Form must be completed prior to removal in accordance with UAMS Administrative Guide Policy 5.4.01, Property Control. This form can be obtained at: http://supplychain.uams.edu/hom/property/forms/ or by contacting Property Services.

VI. Employees and/or supervisors should contact IT to verify software or hardware compliance.

Sanctions

Violation of this Policy will result in disciplinary action in accordance with Administrative Guide Policy 4.4.02, Employee Discipline.

Signature: Daniel W Rahn

Date: **May 6, 2015**