



UNIVERSITY OF ARKANSAS  
FOR MEDICAL SCIENCES

## UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.40

DATE: 04/01/2005

REVISION: 11/15/2006; 02/01/2010; 3/3/2011

PAGE: 1 of 4

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: EMPLOYEES AUTHORIZED TO HAVE WORK STATIONS AT HOME

### 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 employees physicians, 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.

**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 and health information about UAMS employees maintained by UAMS in its role as an employer.

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

- Transmitted by electronic media
- Maintained in electronic media

**Information Systems** 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 part-time or full-time in an official UAMS capacity are responsible for maintaining the privacy and security of all UAMS Confidential Information including Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) and for following all UAMS policies and procedures related to Confidential Information, PHI, and ePHI.

## **PROCEDURE**

1. Confidential Information, including PHI, is only to be removed from UAMS by members of the Workforce when necessary to complete their job duties. Prior approval to work from home must be obtained from their supervisor.
2. 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. Protected Health Information and Electronic Protected Health Information
  - B. Computers that contain or access Confidential Information
  - C. Confidential Working Papers
3. All UAMS policies are in effect whether the Workforce member is working off-site or in a UAMS facility.
  - A. IT Network Security [7.3.08](#)
    1. VPN should be utilized when possible to avoid saving data to home computers. All computer access storing PHI must be encrypted.
    2. Any Confidential Information or ePHI sent from workstations, laptops, PDAs and other mobile devices must be encrypted.
  - B. Safeguarding PHI Policy [3.1.38](#)

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 in an unattended vehicle.
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 and CDs. 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. IT Network Security [7.3.14](#)

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

D. Mobile Device Safeguards [3.1.17](#) and HIPAA Security Protection from Malicious Software [7.3.15](#)

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. All home computers and mobile devices, including thumb drives must be encrypted in accordance with [Policy 3.1.17](#).
2. Employees are required to maintain updates to current operating systems (ex. Microsoft updates/patches)

E. Confidentiality Policy [3.1.15](#)

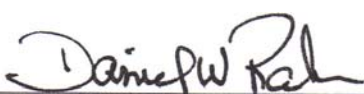
1. Passwords to computers storing confidential information must not be shared or made accessible to family members or others.
2. UAMS passwords must never be shared with anyone.

F. The printing of confidential information from home computers should be kept to a minimum and only as needed in accordance with UAMS policies.

4. UAMS departmental equipment taken home requires a signed UAMS Property Located Off-Campus Form.
5. 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 [Policy 4.4.02](#).

Signature: 

Date: May 11, 2011