



NUMBER: 7.3.09

DATE: 03/24/2005

REVISION: 11/06/2009; 11/02/2011

PAGE: 1 of 3

SECTION: INFORMATION TECHNOLOGY  
AREA: NETWORK SECURITY  
SUBJECT: FACILITY PHYSICAL ACCESS CONTROLS

## PURPOSE

To establish minimum requirements concerning the required physical controls for facilities housing systems containing Protected Health Information (PHI).

## SCOPE

UAMS Workforce

## DEFINITIONS

**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.

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

- Transmitted by Electronic media
- Maintained in Electronic media

**Facility** means the physical premises and the interior and exterior of a building(s).

**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.

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

## **POLICY**

UAMS will create and maintain appropriate access controls to limit physical access to its electronic Information Systems that contain Confidential Information, including (ePHI), and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.

## **PROCEDURES**

**Access Control and Validation:** a person's access to facilities will be based on their role or function, including visitor control and control of access to software programs for testing and revision.

### 1. Workforce Access Controls:

- Workforce member access to all facilities used to house systems containing Confidential Information, including ePHI, will be controlled and validated to the extent necessary.
- UAMS must adopt appropriate access control mechanisms to control physical access to all areas containing systems that incorporate Confidential Information and will have appropriate physical access control mechanisms. Code locks, badge readers, and key locks are examples of physical access control mechanism.
- The request for and management of keys to UAMS facilities will be in accordance with [UAMS Administrative Guide 11.1.4 Key Requests/Transfers](#).
- UAMS Workforce members must wear their UAMS Identification Badges at all times when performing duties on behalf of UAMS.

### 2. Visitor Access Controls:

Visitor access to any area used to house systems containing Confidential Information will be controlled and validated. Visitors include non-UAMS Workforce members such as vendors, outside repair vendors, patients and their families. [Refer also to UAMS Medical Center Patient Visitation Policy PS.2.04](#) for additional information regarding patient visitors.

- All persons (patients, visitors, vendors and others) who are not authorized to have access to ePHI and Confidential Information should be supervised, escorted or observed when visiting or walking through an area where ePHI or Confidential Information may be viewed or accessed easily. Vendors and contractors should wear company ID and/or be provided temporary identification badges issued by UAMS. [Refer also to the UAMS Administrative Guide 4.4.12 Industry Interaction](#).

### 3. Physical Access Record Controls

Physical access to any facility containing high risk, confidential or ePHI based systems including identity and purpose of the visit will be logged.

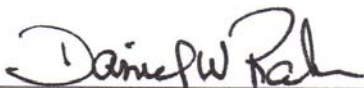
**Facility Security Plan:** procedures to safeguard all facilities, systems, and equipment used to store Confidential Information, including ePHI, against unauthorized physical access, tampering, and theft. Examples include, but are not limited to, physical barriers, utilizing locks, alarms and other access control devices, and providing controls to guard against fire damage, power outages, and other similar occurrences.

**Contingency Operations:** procedures that allow physical facility access during emergencies to support restoration of data under the UAMS Emergency Response Plan (ERP).

**Maintenance Records:** The UAMS Physical Plant and UAMS Police Department will maintain records of repairs and modifications performed by their respective departments to areas housing Confidential Information, including ePHI. All other areas will implement procedures to document repairs and modifications to the physical security components of their facility that house Confidential Information including locks, doors, and other physical access control hardware.

### **SANCTIONS**

Violation of this Policy will result in disciplinary action, in accordance with [Policy 4.4.02](#).

Signature:  \_\_\_\_\_

Date: November 2, 2011