SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: FACILITY PHYSICAL ACCESS CONTROLS

PURPOSE

To establish the University of Arkansas for Medical Sciences' ("UAMS") minimum requirements concerning the required physical controls for Facilities housing systems containing Protected Health Information ("PHI").

SCOPE

The 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 ("ePHI") 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, 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 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.

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

POLICY

UAMS will create and maintain appropriate access controls to limit physical access to its Facility or Facilities where PHI, including PHI in paper format and electronic Information Systems that contain Confidential Information, including ePHI, are housed. The access controls will ensure properly authorized access is allowed.

PROCEDURES

A. 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, upgrades, troubleshooting, and revision.

1. Workforce Access Controls:

    a. Workforce members' access to all Facilities that house systems containing Confidential Information, including ePHI, will be controlled and validated to the extent necessary. Facilities that house information systems containing Confidential Information include, but are not limited to, server rooms, media storage areas, and data communication centers.

    b. 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, alarms, and key locks are examples of physical access control mechanisms.

    c. The request for, and management of, keys to UAMS Facilities will be in accordance with *UAMS Administrative Guide Policy 11.1.4, Key Requests.*

    d. UAMS Workforce members must wear their UAMS identification badges at all times when performing duties on behalf of UAMS.

2. Visitor Access Controls:

    a. 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, Family and Guest Presence Policy PS.2.04* for additional information regarding patient visitors.

    b. 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 Confidential Information,

including PHI in paper format and ePHI, may be viewed or accessed easily.

c. Vendors and contractors should wear company ID and/or be provided temporary identification badges issued by UAMS. *Refer also to the UAMS Administrative Guide Policy 4.4.12, Industry Interaction.*

B. Records of Physical Access to Facilities

Physical access to any Facility containing Confidential Information that is high risk, in paper or electronic format, will be recorded along with the identity of the individual and the purpose of the visit.

C. Damage and Destruction: Safeguards to protect against damage and destruction will be implemented as necessary in Facilities, systems, and equipment used to store Confidential Information, including ePHI. Examples include, but are not limited to, controls to guard against fire damage, power outages, and other similar occurrences.

D. Emergency Operations: Procedures will be implemented that allow physical Facility access during emergencies and other hazardous events to support restoration of data in accordance with the UAMS All Hazards Plan.

E. Maintenance Records: The UAMS Physical Plant will maintain records of repairs and modifications performed to areas housing Confidential Information, including ePHI. UAMS Security Support Services will maintain records of repairs and modifications to locks, badge readers, video surveillance, panic alarms and other such technologies and devices.

SANCTIONS

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

Signature:  **Date: February 9, 2021**