SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: AUDIT CONTROLS FOR CONFIDENTIAL INFORMATION

PURPOSE

To inform the University of Arkansas for Medical Sciences ("UAMS") Workforce about audit controls for Confidential Information.

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

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, applications, communications, and people.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable belief the information could 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, 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.

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.

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

POLICY

UAMS will record and examine significant activity on its Information Systems that contain Confidential Information, including ePHI. Audit mechanisms will be placed on Information Systems that use or contain Confidential Information. UAMS will develop and implement a formal process for audit log reviews and conduct audits regularly. The UAMS HIPAA Office has the authority to conduct audits on any UAMS computer system that contains ePHI.

PROCEDURE

1. Information Systems that contain or use Confidential Information must be able to record and examine potentially unauthorized activity. Risk Analyses will be conducted by Information Technology to identify potentially unauthorized activity on systems as required.

2. Software, hardware or procedural auditing mechanisms will be implemented on UAMS Information Systems that contain Confidential Information. The mechanisms should provide date and time of the potentially unauthorized activity; origin of potentially unauthorized activity; identification of user performing potentially unauthorized activity; and the description of attempted or completed potentially unauthorized activity. If a system does require the use of an auditing mechanism but does not support an auditing mechanism, efforts will be made to upgrade the system within a reasonable time frame.

3. All UAMS information systems containing Confidential Information will be regularly audited for potentially unauthorized activity. Activities to be audited may include but not be limited to the following: Access of certain data; use of certain software programs and utilities; use of a privileged account; Information System start up or stop; and failed Authentication attempts.

4. Audit logs generated by UAMS electronic information systems will be reviewed by system administrators and the HIPAA Office when applicable. Any suspected Security Incidents are to be reported to the Information Technology Security Department (501-686-8555) ITSecurityTechnical@uams.edu to determine any appropriate action. These reports and any response taken must be documented and kept on file for 6 years.

5. All other Security Incidents suspected or known by any member of the UAMS Workforce must be reported on a timely basis to the appropriate person in accordance with the UAMS reporting policy, *Adminstrative Guide Policy 2.1.08 REPORTING OF HIPAA VIOLATIONS*.

6. **Periodic reviews of records of Information Systems activity to minimize security violations to Confidential Information, including ePHI must adhere to the following**

requirements.

a. Records of activity identified for review include but are not limited to:
    i. Audit logs
    ii. Access reports
    iii. Security Incident tracking reports
b. At a minimum, the documented reviews include the following information:
    i. Date and time of the activity
    ii. Origin and significance of the activity
    iii. Identification of user performing activity
    iv. Description of attempted or completed activity
    v. Identification of the reviewer assigned to assess the records of activity
c. The level and type of auditing mechanisms implemented must be determined by a Risk Analysis and reviewed on a regular basis. Auditable events can include but are not limited to:
    i. Access of sensitive data (such as HIV results or PHI of public figures)
    ii. Use of a privileged account
    iii. Information system start-up or stop
    iv. Failed authentication attempts
    v. System upgrades or module changes
    vi. Security Incidents
d. UAMS Workforce members should not monitor or review activity related to their own user account.

SANCTIONS

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

Signature:  **Date: January 11, 2022**

Security Incident Request **Req. # _____**

A. Requesting Party: _____Date: _____

Department:_____Phone:_____

Department Head:_____

Description of Problem

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Department Head:_____Date:_____

Printed Name: _____

IT Security Officer:_____Date:_____

Division Approver:_____Date:_____

Printed Name: _____