SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: INFORMATION TECHNOLOGY RISK ANALYSIS AND RISK MANAGEMENT OF ELECTRONIC SYSTEMS

PURPOSE

To obtain the knowledge necessary to make the determination as to the balance of risks and the secure use of University of Arkansas for Medical Sciences ("UAMS") data.

SCOPE

UAMS Workforce with access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

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

Information System 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 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.

Risk Analysis means a systematic and analytical approach that identifies and assesses risks to the confidentiality, integrity or availability of a covered entity's ePHI. Risk Analysis considers all

relevant losses that would be expected if specific security measures protecting ePHI are not in place. Relevant losses include losses caused by unauthorized use and disclosure of ePHI and loss of data integrity.

UAMS Workforce means physicians, employees, 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.

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

POLICY

UAMS will conduct an accurate and thorough assessment of the potential Risks and Vulnerabilities to the confidentiality, integrity, and availability of Confidential Information, including Protected Health Information (PHI) and ePHI. UAMS will take effective steps to minimize or eliminate any such potential Risks and Vulnerabilities and will continually assess potential Risks and Vulnerabilities by developing, implementing, and maintaining appropriate Security Measures sufficient to reduce Risks and Vulnerabilities to a reasonable and appropriate level. Selection and implementation of Security Measures are based on a formal, documented Risk management process and must address the confidentiality, integrity and availability of UAMS Information Systems.

PROCEDURE

A. Risk Analysis: At a minimum, the UAMS Risk Analysis process will be based on the following steps:

1. Inventory of systems containing Confidential Information, including ePHI, and Security Measures protecting such systems;
2. Threat and Vulnerability Identification and Prioritization including regular reviews and security assessments;
3. Security Control Analysis including both preventive and detective controls;
4. Risk Likelihood Determination that assigns ratings to specific Risks that include Threat motivation and capability, type of Vulnerability, and existence and effectiveness of current security controls; and
5. Impact and Risk Analysis to determine the impact to confidentiality, integrity or availability that would result if a Threat were to successfully exploit Vulnerabilities on UAMS systems and the adequacy of planned or existing security controls.

In addition to regular Risk Analysis, UAMS will conduct a Risk Analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific Information Systems containing Confidential Information, including ePHI. Such changes include but are not limited to:

1. Significant Security Incidents
2. Significant new Threats or Risks

3. Significant changes to organizational or technical infrastructures
4. Significant changes to UAMS information security requirements or responsibilities

B. Risk Management: At a minimum, the UAMS Risk Management process will be based on the following steps:

1. Inventory of UAMS systems and their Security Measures;
2. Risk Prioritization on a scale from high to low based on the potential impact to systems containing Confidential Information, including ePHI, and the probability of occurrence;
3. Method Selection to minimize or eliminate identified Risks to UAMS systems. Selections must be based on the nature of a specific Risk and the feasibility and effectiveness of a specific method;
4. Cost-benefit Analysis to identify the costs and benefits of implementing or not implementing specific security methods for reducing Risks to systems containing Confidential Information;
5. Assignment of Responsibility to Workforce members who have the appropriate expertise for implementing selected security method(s); and
6. Regularly Scheduled Security Method Evaluations are conducted as needed when performing an upgrade, acquisition, and internal system development life cycle (SDLC).

Signature:  **Date: February 23, 2024**