PURPOSE

To inform the UAMS workforce about the procedures for information access management.

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 and student information, information concerning 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. Confidential Information includes information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

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

- Transmitted/Received by Electronic media
- Maintained in Electronic media

Health Care Operations is defined by the HIPAA regulations under 45 C.F.R. § 164.501 and is incorporated herein by reference, and includes the following:

1. Quality assessment and improvement, including outcomes evaluation and development of clinical guidelines; population-based activities relating to improving health or reducing health care costs, protocol development, case management and case coordination, contacting providers and patients with information about treatment alternatives; and related functions that do not include treatment.
2. Accreditation, certification, licensing or credentialing activities, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals.
3. Conducting or arranging for medical review, legal services and auditing.

4. Business planning and development related to managing and operating the entity. Business management and general administrative activities, such as fundraising and marketing of services to the extent permitted without Authorization, disclosure of PHI in a due diligence review or to resolve internal grievances, and customer service.

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.

Payment includes billing, reimbursement, and collection activities relating to the provision of health care to an individual, including but not limited to, release to an insurance company, insurance plan or other third-party payer in connection with payment activities, eligibility or coverage determinations, disclosures to consumer reporting agencies, health care data processing, claims management and other activities as defined by 45 C.F.R. § 164.501 under "payment."

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 and health information regarding a person who has been deceased for more than 50 years.

Treatment is providing, coordinating or managing health care and related services by one or more providers, including such coordination or management by a provider with a third party; consultation between providers relating to a patient or the referral of a patient for health care from one provider to another.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, residents, trainees, visting 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.

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

POLICY

Access to UAMS Information Systems is managed to protect the confidentiality, integrity and availability of Confidential Information, including ePHI.

UAMS will maintain a documented process for establishing, granting, and modifying access to

Information Systems that contain Confidential Information that must be approved by IT Security.

Access to Confidential Information, including ePHI, is authorized on a "need-to-know" basis in order for the UAMS Workforce to accomplish the work responsibilities of their specific job functions. (*Administrative Guide Policy 2.1.10**,** Minimum Necessary Policy*)

UAMS Information Systems will (where provided by the vendor) allow for unique user identification to identify and track the information system activity of each Workforce member for the purpose of access control to all UAMS networks, systems, applications, and databases that contain Confidential Information, including ePHI. This policy sets forth the procedures established to obtain necessary ePHI or Confidential Information in an emergency. This policy sets forth electronic procedures to protect ePHI by terminating electronic sessions after a specific term of inactivity. UAMS Workforce members transmitting ePHI are responsible for utilizing an encryption mechanism between the sending and receiving entities.

PROCEDURE

ACCESS AUTHORIZATION, ESTABLISHMENT AND MANAGEMENT:

A. This policy sets forth the process of determining who is granted access to the Confidential Information, including ePHI, and who grants this access, which will include, but is not limited to the following:

   1. Procedures for granting different levels of access to UAMS Information Systems;

   2. Procedures for tracking and logging authorization of and access to UAMS Information Systems, including those containing Confidential Information;

   3. Procedures for modifying UAMS Workforce members' access privileges to UAMS Information Systems.

   4. The above procedures must be under the direct control of or approved by IT Security.

B. Formally designated UAMS Information Systems owners or their designees must define and authorize access to UAMS Information Systems containing Confidential Information. The names of the system owners and designees should be documented and on file with IT Security.

C. For purposes under UAMS Treatment, Payment and Healthcare Operations, only authorized UAMS Workforce members or workforce members of Business Associates may access UAMS Information Systems containing Confidential Information, including ePHI, and the access process should be documented. For purposes of UAMS Treatment, Payment and Healthcare Operations, non-Workforce members must receive approval from IT Security before being able to access UAMS Information Systems containing Confidential Information, including ePHI. UAMS Workforce members must not attempt to gain access to UAMS Information Systems for which they have not been given proper

authorization.

D. Security controls or methods that allow access to UAMS Information Systems containing Confidential Information, including ePHI, must at a minimum, include:

1. The prompt removal or disabling of access for persons and entities that no longer need access to the information by managers and via the check-out process; See *Administrative Guide Policy 2.1.30, Information Access for Transfers and Terminations*.
2. The instruction of Workforce members on how to access assigned Information Systems.
3. The instruction to Workforce members not to provide access to UAMS Information Systems containing Confidential Information to any unauthorized persons.
4. Regular review of system users to ensure access for all users is appropriate.

E. Revisions to access rights should be tracked and logged. At a minimum, such tracking and logging must provide:

1. Date and time of revision;
2. Identification of Workforce members whose access is being revised;
3. Brief description of revised access right(s);
4. Reason for revision; and
5. Name of UAMS system owner(s) or designee processing the revision request.

ACCESS CONTROLS FOR CONFIDENTIAL INFORMATION:

A. Unique User Identification and Password:

All UAMS Workforce members that require access to any network, system, or application that accesses, transmits, receives, or stores Confidential Information, must be provided with a unique user identification and password. User identification and password are then necessary to access the area containing Confidential Information. (See *Administrative Guide Policy 2.1.01, Confidentiality Policy*) (See *Administrative Guide Policy 2.1.37, Information Security & Password Management*)

B. Emergency Access:

If the UAMS information system used to provide patient treatment contains ePHI and denial or strict access to that ePHI could inhibit or negatively impact patient treatment, then access to that ePHI must be available to any authorized caregiver on an emergency basis. Each department must establish and implement procedures to ensure emergency access to necessary ePHI is maintained.

C. Automatic Logoff:

1. Servers, workstations, or other computer systems containing ePHI repositories that

have been classified as high risk or are located in open, common, or otherwise insecure areas must employ inactivity timers or automatic logoff mechanisms. Applications and databases using ePHI must employ inactivity timers or automatic session logoff mechanisms.

2. Information Systems should have the capability of terminating user sessions after a period of time as determined appropriate by IT Security. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, efforts will be made to resolve the issue.

3. When leaving a server, workstation, or other computer system unattended, UAMS Workforce members should lock the workstation or logout of all applications and database systems containing Confidential Information.

D. Encryption and Decryption:

1. All Transmissions of ePHI from UAMS to an outside network must utilize an encryption mechanism between the sending and receiving entities, or the file, document, or folder containing ePHI must be encrypted before transmission.

2. Any use of Email to transmit Confidential Information, including ePHI, with other physicians, health care providers, health care associations, or patients must be encrypted. This can be accomplished with any method agreeable to both parties sending and receiving the transmission. UAMS provides an enterprise email encryption solution. (*See Administrative Guide Policy 2.1.31, Email Access and Usage Policy*)

3. All Remote Access to UAMS will be through RAS or VPN Connections. (See *Administrative Guide Policy 7.2.11, Access to Internet*).

E. Security Logon Monitoring:

1. UAMS will implement and maintain a process for monitoring login attempts to UAMS electronic Information Systems that have the capability for logging.

    a. Login information will be validated only when both the username and password have been entered correctly. If an error arises, the system must not indicate which part of the data is correct or incorrect.
    b. Number of unsuccessful login attempts will be limited.
    c. All login attempts will be recorded.

2. UAMS domain login process allows for:

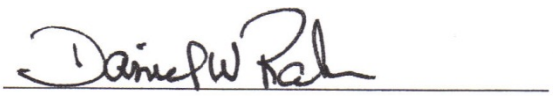
    a. Displaying a notice that access is limited to authorized users.
    b. Recording unsuccessful login attempts.

c. Enforcement of a time delay after a specific number of failed login attempts before further login attempts are allowed, or rejection of any further attempts without authorization from an appropriate UAMS employee.
d. Limits on the maximum time allowed for the login procedure.

3. UAMS Workforce is responsible for reporting suspected login discrepancies to the UAMS Technical support Center at (501) 686-8555 or IT designee.

References:

Administrative Guide Policy 2.1.37, Information Security & Password Management
Administrative Guide Policy 2.1.40, Enterprise Data Integrity & Encryption

Signature: 

Date: November 6, 2013