



NUMBER: 7.3.04

DATE: 03/24/2005

REVISION: 4/24/2008

PAGE: 1 of 3

SECTION: INFORMATION TECHNOLOGH
AREA: NETWORK SECURITY
SUBJECT: INFORMATION ACCESS MANAGEMENT

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 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.

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.

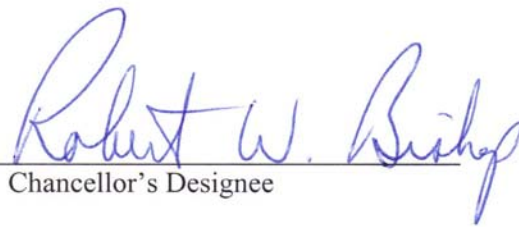
Access to Confidential Information, including ePHI, is authorized on a “need-to-know” basis in order for the UAMS Workforce to accomplish the work responsibilities of their specific job functions. ([UAMS Policy 3.1.25 Minimum Necessary](#))

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.
- 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. Only authorized UAMS Workforce members may access UAMS Information Systems containing Confidential Information, including ePHI, and the access process should be documented. 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;
 2. The instruction of Workforce members on how to access assigned Information Systems; and,
 3. The instruction to Workforce members not to provide access to UAMS Information Systems containing Confidential Information to any unauthorized persons.
- 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.

SIGNATURE: _____


Chancellor's Designee

DATE: April 24, 2008