



UNIVERSITY OF ARKANSAS
FOR MEDICAL SCIENCES

UAMS ADMINISTRATIVE GUIDE

NUMBER: 7.3.14

DATE: 04/01/2005

REVISION: 4/24/2008

PAGE: 1 of 3

SECTION: INFORMATION TECHNOLOGY

AREA: NETWORK SECURITY

SUBJECT: ACCESS CONTROLS FOR CONFIDENTIAL INFORMATION

PURPOSE

To inform the UAMS workforce about access controls for confidential information.

SCOPE

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.

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

A. Unique User Identification and Password:

1. 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 [UAMS Confidentiality Policy 3.1.15](#)) (See [UAMS Information Security & Password Management Policy 7.3.08](#))

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.

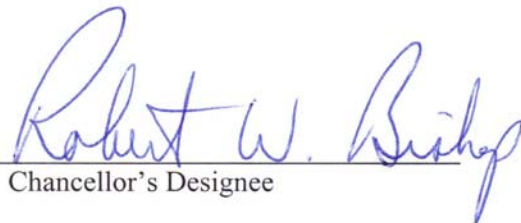
C. Automatic Logoff:

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 maximum of ten minutes of user inactivity. 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 [UAMS Email Access and Usage Policy 7.1.12](#))
3. All Remote Access to UAMS will be through RAS or VPN Connections. (See [UAMS Remote Access Service to UAMS Network Policy 7.2.10](#))

SIGNATURE: _____


Chancellor's Designee

DATE: April 24, 2008