



NUMBER: 7.3.07

DATE: 03/24/2005

REVISION: 02/01/2010; 12/14/2011

PAGE: 1 of 2

SECTION: INFORMATION TECHNOLOGY

AREA: NETWORK SECURITY

SUBJECT: SECURITY LOG-IN MONITORING

PURPOSE

Notify UAMS Workforce of procedures implemented to protect user Log-ons.

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.

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.

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

POLICY

UAMS will implement and maintain a process for monitoring log-in attempts to the UAMS electronic Information Systems and for reporting discrepancies.

PROCEDURE

- A. All UAMS Information Systems must be accessed through a secure log-in.
 - 1. Log-in information will be validated only when all data has been entered. If an error arises, the system must not indicate which part of the data is correct or incorrect.
 - 2. Number of unsuccessful log-in attempts will be limited.
 - 3. All log-in attempts will be recorded.

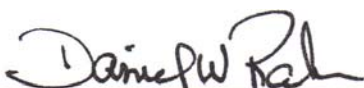
- B. UAMS domain log-in process allows for:
 - 1. Displaying a notice that access is limited to authorized users.
 - 2. Recording unsuccessful log-in attempts.
 - 3. Enforcement of a time delay after a specific number of failed log-in attempts before further log-in attempts are allowed, or rejection of any further attempts without authorization from an appropriate UAMS employee.
 - 4. Limits on the maximum time allowed for the log-in procedure.

- C. UAMS Workforce is responsible for reporting suspected log-in discrepancies to the UAMS Technical Support Center at (501) 686-8555 or IT designee.

REFERENCES

[*UAMS Admin Guide Malicious Software Protections Policy 7.3.15*](#)

[*UAMS Admin Guide Information Security Password Management Policy 7.3.08*](#)

Signature: 

Date: December 14, 2011