UAMS
UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES

**UAMS ADMINISTRATIVE GUIDE**

**NUMBER: 2.1.30** **DATE: 04/01/2005**
**REVISION: 01/11/2011; 01/02/2013** **PAGE: 1 of 3**
**SECTION: HIPAA**
**AREA: HIPAA PRIVACY/SECURITY POLICIES**
**SUBJECT: INFORMATION ACCESS FOR TRANSFERS AND TERMINATIONS**

## PURPOSE

This policy is established to safeguard the privacy and security of our patients' Protected Health Information by setting the guidelines for all UAMS Workforce members who terminate employment or transfer within UAMS.

## 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

**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, for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are 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 IT Security will implement procedures to ensure that UAMS Workforce members are granted appropriate access to ePHI. When a UAMS workforce member's employment ends or a determination is made that such access no longer is needed, any existing PHI will be retrieved from the Workforce member and access to ePHI will be terminated. (*Administrative Guide Policy 2.1.01, Confidentiality Policy*) UAMS IT Security processes the termination of all employees in accordance with the *Administrative Guide Policy 4.5.16, Employee Separation Procedure.*

## PROCEDURE:

These procedures help ensure the timely disabling of UAMS network and information system account(s) and the removal of physical access to UAMS facilities.

**A.** Departments are responsible for updating employee status (transfers or terminations) in the UAMS Financial System (SAP) on a timely basis.

**B.** When employees separate from UAMS, all access to our systems must be terminated. To facilitate a rapid disabling of all accounts, a check box is included on the UAMS Employee Separation Form. It is called "Institutional Compliance" (location Central Hospital, 1st Floor, under Items Section "Computer Access (all employees)".

1. As part of the check out process, the terminating employee must report to the HIPAA Office to have a staff member sign off and date in the appropriate box.
2. If the employee is transferring, this form should also be used. Under "Reason for Separation" the "transfer to" line should be checked with the appropriate reason on the line provided. Only the domain access will remain available to the transferring employee until the receiving department determines the employees level of access for that new position.
3. HIPAA staff will verify that the employee does not have PHI in their possession, at home, on electronic devices or elsewhere.
4. After signing the Employee Separation Form, the HIPAA Office notifies IT Security to disable, or in the case of a transferring employee, modify the employee's access as soon as possible.

**C.** The UAMS Financial System (SAP) will send a list of all UAMS workforce terminations (voluntarily or involuntarily) to IT Security. When the employment of a UAMS workforce member ends, their information systems privileges, both internal and remote, will be disabled. If the employee is dismissed involuntarily, it is the supervisor's responsibility to ensure compliance with these actions.

**D.** As an additional safeguard, UAMS disables a user account after ninety (90) days of inactivity and automatically deletes it after 120 days of continuous inactivity.

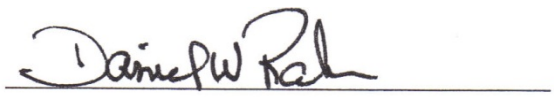
**E.** Department supervisors are responsible for reviewing transferring employees' computer access levels and notifying the Department's IT Administrator or the UAMS IT Security Office (either by e-mail, phone call (501-526-6028) or by completing the IT System Access Form) of any computer system access levels that must be maintained, assigned or deactivated.

**F.** Physical access to UAMS facilities after termination or transfer. Please refer to *Administrative Guide Policy 11.1.04 Key Requests* for additional details.

1. Terminations: Upon separation from UAMS, physical access to UAMS facilities is also terminated. As a part of the clearance procedure, faculty and staff shall return all keys to the Physical Plant Key Office and their ID Badge to Campus Police.
2. Transferring work force members: Direct key transfers to other employees are not permitted. All keys must be returned to the Physical Plant Key Office by the person to whom they were issued.
3. The Department of the terminating or separating employee will notify the Physical Plant Key Office if a determination is made that locks need to be re-keyed or combinations changed.

## SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with *Administrative Guide Policy 4.4.02, Employee Discipline*.

Signature: 

**Date: January 2, 2013**