



UNIVERSITY OF ARKANSAS  
FOR MEDICAL SCIENCES

## UAMS ADMINISTRATIVE GUIDE

NUMBER: 7.3.05

DATE: 03/24/2005

REVISION: 4/24/2008

PAGE: 1 of 3

**SECTION: INFORMATION TECHNOLOGY**  
**AREA: NETWORK SECURITY**  
**SUBJECT: INFORMATION SYSTEM ACTIVITY REVIEW**

---

### PURPOSE

To inform the UAMS workforce about information system activity reviews.

### 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.

To access any other terms or definitions referenced in this policy:

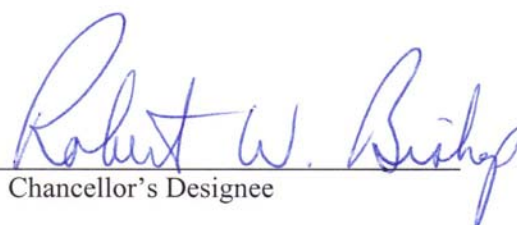
<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

**POLICY:**

UAMS conducts periodic internal reviews of records of Information Systems activity to minimize security violations to Confidential Information, including ePHI. UAMS assesses potential risks and vulnerabilities to Confidential Information, including ePHI, and develops, implements, and maintains appropriate administrative, physical, and technical security measures in accordance with good business practices and any applicable regulations, including the HIPAA Security Regulations.

- A. Records of activity identified for review include but are not limited to:
  - 1. Audit logs
  - 2. Access reports
  - 3. Security Incident tracking reports
  
- B. At a minimum, the documented reviews include the following information:
  - 1. Date and time of the activity
  - 2. Origin and significance of the activity
  - 3. Identification of user performing activity
  - 4. Description of attempted or completed activity
  - 5. Identification of the reviewer assigned to assess the records of activity
  
- C. The level and type of auditing mechanisms implemented must be determined by a Risk Analysis and reviewed on a regular basis. Auditable events can include but are not limited to:
  - 1. Access of sensitive data (such as HIV results or PHI of public figures)
  - 2. Use of a privileged account
  - 3. Information system start-up or stop
  - 4. Failed authentication attempts
  - 5. System upgrades or module changes
  - 6. Security Incidents
  
- D. UAMS Workforce members should not monitor or review activity related to their own user account.

SIGNATURE: \_\_\_\_\_

  
Chancellor's Designee

DATE: April 24, 2008

