



UNIVERSITY OF ARKANSAS
FOR MEDICAL SCIENCES

UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.15

DATE: 03/05/2002

REVISION: 06/06/2006, 4/24/2008, 9/23/2009; 9/8/2011

PAGE: 1 of 5

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: CONFIDENTIALITY POLICY

PURPOSE

To inform the UAMS Workforce about the UAMS Confidentiality Policy.

SCOPE

UAMS Workforce as well as non-UAMS employees, vendors, consultants and other visitors who may access Confidential Information.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee and student information, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information includes Protected Health Information. Confidential Information includes information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

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: UAMS Workforce includes UAMS 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 prohibits the unlawful or unauthorized access, use or disclosure of Confidential Information obtained during the course of employment or other relationship with UAMS. As a condition of employment, continued employment or relationship with UAMS, the UAMS workforce and all non-UAMS employees, vendors, consultants and other visitors who may access Confidential Information shall be required to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General Counsel ([Appendix A](#)). UAMS will provide training for each of its workforce members on the importance of maintaining confidentiality and the specific requirements of state and federal law, including the HIPAA Privacy Regulations and laws protecting the privacy of students and employees, as well as UAMS policies, in accordance with [Policy 3.1.30 HIPAA Education and Training](#).

PROCEDURES:

1. **Confidentiality Agreement:** As a condition of employment, continued employment, or relationship with UAMS, UAMS will require its workforce and all non-UAMS employees, vendors, consultants and other visitors who may access Confidential Information to sign the UAMS Confidentiality Agreement.

All new employees, students, or vendors requiring access to electronic Confidential Information (computer systems) must have a current Confidentiality Agreement on file in the IT Security Office. The person signing the agreement will receive a copy of the Confidentiality Policy with the Confidentiality Agreement. The UAMS IT Security Office will maintain signed Confidentiality Agreements. It is the responsibility of the manager or of the hiring individual vendors or consultants (who do not require electronic access but who may have access to Confidential Information) to require execution of the appropriate confidentiality agreements approved by the UAMS Office of General Counsel and to send those documents to the UAMS IT Security Office.

2. **Restriction on Access, Use and Disclosure of Confidential Information:** UAMS limits and restricts access to Confidential Information and computer systems containing Confidential Information based upon the specific job duties and functions of the individual accessing the information. UAMS will restrict access to Confidential Information to the minimum necessary to perform individual job functions or duties. UAMS will further limit and control access to its computer systems with the use of unique sign-on and password codes issued by the IT Security Office to the individual user authorized to have such access. Users are prohibited from sharing their password or using the access codes of another.

Authorization to access, use or disclose Protected Health Information also is governed by the [UAMS Use and Disclosure Policy 3.1.28](#).

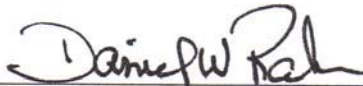
UAMS will control and monitor access to Confidential Information through management oversight, identification and authentication procedures, and internal audits. UAMS managers and heads of departments will have the responsibility of educating their respective staff members about this Policy and the restrictions on the access, use and disclosure of Confidential Information, and will monitor compliance with this Policy.

3. **Sales Representatives and Service Technicians:** Sales representatives and service technicians must register in the appropriate area and execute the Confidentiality Agreement prior to any exposure to UAMS Confidential Information.
4. **Media:** All contacts from the media regarding any Confidential Information must be referred to the UAMS Office of Communications and Marketing (501-686-8998 or pager 501-395-5989).
5. **Violation of Confidentiality Policy:** Individuals shall not access, use, or disclose Confidential Information in violation of the law or contrary to UAMS policies. Each individual allowed by UAMS to have access to Confidential Information must maintain and protect against the unauthorized access, use or disclosure of Confidential Information. Any access, use or disclosure of Confidential Information in any form – verbal, written, or electronic – that is inconsistent with or in violation of this Policy will result in disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic program, loss of privileges, or termination of relationship with UAMS. Any workforce member whose relationship with UAMS is not terminated as a result of violating this Policy must, in order to continue working at or attending UAMS, complete a HIPAA training module through the UAMS HIPAA Office.

All UAMS employees and others subject to this Policy must report any known or suspected incidents of access, use or disclosure of Confidential Information in violation of this Policy or in violation of the law to the [HIPAA Office](#) at 603-1379, in accordance with [Policy 3.1.23 Reporting Policy for HIPAA Violations](#).

SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with [Policy 4.4.02 Disciplinary Notice Policy](#).

Signature: 

Date: September 8, 2011

CONFIDENTIALITY AGREEMENT

As a condition of my employment, continued employment or relationship with UAMS, I agree to abide by the requirements of the UAMS Confidentiality Policy and with federal and state laws governing confidentiality of a patient’s Protected Health Information, and I agree to the terms of this Confidentiality Agreement. I understand and agree that the confidentiality laws require me to maintain the confidentiality of this information even when I am not at work or acting within the scope of my relationship with UAMS and also after my employment or relationship with UAMS ends.

I understand and agree that if I access, use or disclose Confidential Information in any form – verbal, written, or electronic – in a manner that is inconsistent with or in violation of the Confidentiality Policy, UAMS may impose disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic program, loss of privileges, or termination of relationship with UAMS.

I understand that when I receive a sign-on code to access the UAMS Network and Systems, I have agreed to the following terms and conditions:

- The sign-on and password codes assigned to me are equivalent to my signature, and I will not share the passwords with anyone.
- I will not attempt to use or share the passwords of another.
- I will be responsible for any use or misuse of my network or application system sign-on codes.
- I will not attempt to access information on the UAMS Network and Systems except to meet needs specific to my job or position at UAMS.

I acknowledge that I have read the terms of this Confidentiality Agreement, and that I have received a copy of the Confidentiality Policy.

_____ *Last four digits of SS#* _____
(Signature)

Print Full Name: _____

Date: _____ Department: _____

Witness at UAMS Orientation only, otherwise not required: _____

Supervisor/Manager’s Signature: _____ Date: _____

(If Vendor, then Department Head Signature required)

Department Head Signature: _____ Date: _____

(Please return completed form to UAMS IT Security Office, #802, Fax 501-603-1369)

FOR NON-UAMS EMPLOYEES (Not loaded into SAP), VENDORS & CONSULTANTS ONLY

Please provide the following additional information:

1. UAMS Sponsor Name/Title: _____

Department: _____

2. What type of access is needed: _____ On-Site _____ Remote

Describe: _____

3. Please describe why the access is needed: _____

For non-UAMS employees requiring access to electronic systems i.e. email; the 'sponsor' should contact their department head to coordinate SAP processing.