



NUMBER: 2.1.34

DATE: 10/31/2002

REVISION: 9/21/2007; 6/23/2010; 02/08/2012; 03/05/2014; 05/07/2014 PAGE: 1 of 4

SECTION: HIPAA

AREA: HIPAA PRIVACY/SECURITY POLICIES

SUBJECT: COMPUTER DEVICE CUSTODIAL PRACTICES TO PROTECT
CONFIDENTIAL INFORMATION

PURPOSE

To inform the UAMS workforce about secure practices to protect confidential information on computer devices.

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.

Mobile Devices are defined as Personal Digital Assistants (PDAs), tablets, cellular phones, text pagers, laptop computers, and any other types of mobile devices or media that receive, record or store information and data.

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, health information about UAMS employees maintained by UAMS in its role as an employer and health information regarding a person who has been deceased for more than 50 years.

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:

POLICY

UAMS is committed to protecting the confidentiality of information (Protected Health Information, confidential research data, and confidential employee and student records) maintained on UAMS computer devices and to prohibit unauthorized access to such information. Systems through which confidential information may be accessed must be protected through the following procedural UAMS workstation custodial practices. These practices facilitate compliance with related federal and state statutes and regulations. This policy applies equally to all devices through which confidential information and PHI may be accessed or distributed.

PROCEDURE

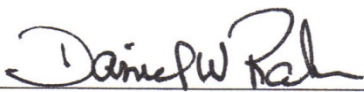
1. **Placement of Workstations (including printers and data entry/display terminals):** The placement of data entry/display terminals and printers on which confidential information or PHI may be accessed or displayed is evaluated as part of the IT Project Plan under which the devices will be implemented. Placement is evaluated a second time, upon installation by IT Workstation Support. After installation each UAMS department is responsible for continued monitoring of placement changes.
2. **Automatic Log-off Intervals:** All software systems through which PHI is accessible are required to have an automatic logoff. Any exceptions must be approved by IT Security. Logoff intervals are determined by UAMS IT Security in conjunction with each department and reviewed annually for compliance and revisions.
3. **Activating and Deactivating Passwords:**
 - A. UAMS staff and students and all other persons requesting access to non-public resources available on the UAMS network domain must review and sign a UAMS Confidentiality Agreement prior to being granted access. UAMS Colleges may include the Confidentiality Agreements for students as a component of a set of policies provided to students for which they must acknowledge by signature agreement.
 - B. Assignment of passwords to systems or data bases containing PHI must be administered by IT Security or through an IT Security approved process.
 - C. All information systems through which PHI is accessible must employ some form of access security using passwords, biometrics, tokens, or other techniques.
 - D. UAMS departments are responsible for terminating within SAP all persons who leave the employ of UAMS. UAMS IT Security will generate an exiting employee report each business day and deactivate all accounts having access to systems through which PHI is accessible. UAMS domain accounts will be disabled automatically in a daily process.
 - E. Supervisors are responsible for notifying IT regarding all involuntary terminations.

- F. Departments are responsible for updating employee status (job change or termination) in SAP on a timely basis.
 - G. 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 email, phone call or by completing the IT System Access Form) of any computer system access levels that must be maintained, assigned or deactivated.
4. **Workstation Access:** Access to workstations through which confidential information and PHI is accessible is granted to authorized individuals on a need-to-know basis. Persons authorized to use confidential information and PHI in their official UAMS duties are required to safeguard that information and may use it only for, and to the extent required by, official UAMS business purposes. Authorized PHI users must not in any way further disclose or provide that information to others except in accordance with UAMS policies and procedures.
5. **User Education:**
- A. UAMS employees and students are educated on information security at time of orientation.
 - B. Non-employees or vendors requesting access to systems containing PHI must be approved by IT Security and will only be granted in accordance with UAMS Policy and are required to be sponsored by a UAMS department, provided access to the UAMS Confidentiality Policy, and sign the UAMS Confidentiality Agreement before being granted access to any UAMS computer system. Non-employees and vendors should be entered into SAP as a "non-employee" by the sponsoring department for automatic domain account creation. *See Administrative Guide Policy 2.1.18, Business Associate Policy.*
 - C. All persons who will be granted access to information systems through which Confidential Information or PHI is accessible must complete training, as required, for use of those systems.
6. **Physical Security:** PCs, mobile devices, or any other device containing confidential information or PHI must be secure. *See Administrative Guide Policy 2.1.02, Mobile Device Safeguards.* Also refer to *Administrative Guide Policy 2.1.23, Safeguarding Protected Health Information.* All PHI and other confidential information generated at UAMS is considered to be the property of UAMS and is not to be removed without prior approval.
7. **Termination:** Upon employee termination from UAMS, users of any personally owned computers and other mobile devices are responsible for permanently removing all UAMS confidential information and UAMS owned software from the device(s). The employee should coordinate with their supervisor the removal of any PHI on UAMS owned computers or mobile devices.

8. Departments are responsible for maintaining an inventory of all computers, laptops, smart phones and other mobile devices. If a Device containing Confidential Information is lost or stolen, or if you suspect someone has improperly used or accessed protected information on your Mobile Device, it must be reported immediately (24/7) to the UAMS IT Security Officer by calling (501) 686-8555 and applicable law enforcement. Immediate reporting may allow for mitigation of a potential breach.

SANCTIONS

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

Signature: 

Date: May 7, 2014