SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: INFORMATION SECURITY & PASSWORD MANAGEMENT

PURPOSE

A great amount of sensitive data resides on UAMS computer systems, including patient, physician, education, research, and employee information. As a result, all UAMS system users must assume responsibility for the security, accuracy and integrity of the data to which they have access. Authorized access to this information is a privilege granted to assist in performance of work functions.

SCOPE

UAMS Workforce

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee and student 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. Confidential Information includes information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

Electronic Protected Health Information means individually identifiable health information that is:

- Transmitted/Received 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 and health information regarding a person who has been deceased for more than 50 years.

Software means for the purpose of this policy programs, purchased or developed by individuals in the employment of UAMS.

UAMS Workforce means for purposes of this Policy, 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

Access to information and systems must be restricted to a need-to-know basis. Users are responsible for the security of their passwords and all data which they are authorized to access. All UAMS data and documentation is confidential, and must not be taken elsewhere when an employee, student, consultant, or contractor is no longer employed by, enrolled at, or under contract with UAMS. For workstations and laptops, the primary user of that system is responsible for backups and any other measures necessary to insure the security and integrity of the data and software stored locally. For network file servers, the Network Administrator is responsible for the backups and other measures necessary for the overall security of the software and data stored on the network storage space. All users on the network are encouraged to store important data on the network file servers.

PROCEDURE

1. The personal computers and software belong to UAMS and must be used in accordance with UAMS policy. Each campus department shall determine individual computer use.

2. The use and/or copying of software shall be governed by license agreement. Illegal copying or distribution of software is strictly prohibited.

3. All UAMS personal computers and laptops must have approved virus protection software installed and operational, require passwords for any use beyond acting as a portal, and be encrypted by an approved method or waived where appropriate. Personally owned computers and laptops that store UAMS confidential information must also be password-protected and encrypted, unless an encryption-waiver is obtained.

4. Products obtained from open source services or shareware and public domain products must be checked for viruses prior to installation on UAMS personal computers and such products must be related to official UAMS business.

5. Inbound modem access is prohibited on networked workstations. Individual modems must be configured as outbound only. Inbound calls must be routed through the UAMS Secure Inbound modem pool. Individual exceptions may be granted by the Information

Technology Steering Committee if a specific need is present and adequate security is provided.

6. Computer resources utilizing wireless technology must follow guidelines set forth in *Administrative Guide Policy 7.1.13 Wireless Networking*.

7. UAMS E-mail is the property of UAMS. UAMS e-mail must not be used for commercial business purposes, to send inappropriate or offensive materials (such as chain letters, pornography, SPAM), or to send threatening messages. Messages may not be broadcast to "Everyone" within UAMS without prior permission from the UAMS e-mail administrator and non-UAMS function announcements will not be approved. See *Administrative Guide Policy 2.1.31, E-mail Access and Usage* for additional information.

8. UAMS will maintain a formal, documented process for appropriately creating, changing, reviewing and safeguarding passwords used to validate a user's identity and establish access to its information systems and data.

9. UAMS Password Management system will:

   A. Where appropriate, require the use of individual passwords to maintain accountability. Passwords must never be shared among users.

   B. For systems that have capability, require unique passwords that must be a minimum of 8 characters and should be a combination of alphabetic, special, and numeric characters. Password phrases or sentences of 12 characters or more are highly recommended for the UAMS domain log-in. Passwords should also be changed periodically as a matter of good user practice. When changing a password, the new password must not be the same as the current or previously used password. Domain log-in accounts will be subject to scheduled password changes at least every 120 days. Passwords should not be based on something that can be easily guessed or obtained using personal information. (e.g. names, favorite sports team, etc.)

   C. Require passwords to be concealed as they are entered into the applications or systems.

   D. Require passwords to be given to users in a secure and confidential manner.

10. Programs used to automatically log intelligent workstations onto the host must not contain hard-coded passwords. Automated log-on programs are acceptable provided the user is prompted for the password at initial log-on time and the password is not permanently stored for further use.

11. UAMS Workforce password management training and awareness shall include, but not be limited to the following required procedures:

    A. The importance of keeping passwords confidential.

B. The avoidance of maintaining a paper record of passwords.

C. The changing of passwords whenever there is any indication of possible compromise.

D. The importance of not using the same password for personal and business accounts.

E. The requirement of changing passwords at regular intervals and limitations of re-using old passwords on domain log-in accounts.

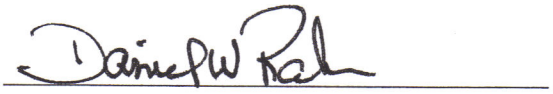
F. The changing of temporary passwords at the first log-on.

G. The importance of not including passwords in any automated log-on process.

H. The responsibility of UAMS Workforce members to maintain and use their password in a secure and confidential manner.

SANCTIONS

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

Signature: 

Date: October 2, 2013