



UAMS

HIPAA HYPE

"Confidentiality is everyone's job,
not everyone's business."



January, 2007

In this issue:

- Password Management
- Securing Mobile Devices

Password Management

UAMS policies [3.1.15-Confidentiality](#) and [7.3.08-Information Management and Password Security](#) require all members of our workforce to access UAMS electronic information through a secure login process. Choosing a good password and keeping it secure are two very important steps you can take to protect electronic protected health information (ePHI) and other confidential information at UAMS.

When selecting a strong password consider the following guidelines:

- Passwords must be a minimum length of six characters.
- Compose a password based on something that is not personal information so that it cannot be easily guessed. For instance, do not use the names of family members or pets.
- Passwords should be a mix of alphabetic and numeric characters (Examples: #4Gh1b or jOke51mn).
- At UAMS, you are allowed up to 240 characters for a password. Creating a password phrase can be a fun and creative way to make your computer more secure (Examples: "The sky is blue and orange but never on Sunday" or "Frankly my friend I don't give a darn").

Always be aware of the following when keeping your password secure:

- Your password belongs to you. You should never share it with anyone.
- Never use someone else's username or other login information when accessing computer systems. If someone else uses YOUR login to access any UAMS electronic information, YOU will appear as the user on access logs.
- It is a good practice to change your password if you suspect any problems.

- If you suspect inappropriate access with your login and password, notify the IT security department immediately. They can be reached at 501-686-6207.
- Avoid maintaining a paper record of passwords.
- Do not use the same passwords for personal and business accounts.
- Change passwords at regular intervals (90 days) and limit reusing old passwords.

Securing Mobile Devices

UAMS Policy [3.1.17-Mobile Device Safeguards](#) requires that Mobile devices including laptops, Blackberries, personal digital assistants (PDA's) and any other instrument which can receive, store, and transmit ePHI or confidential information must use that device's password protection or 'lock out' feature. Mobile devices must be stored in a secure manner and must not be left in unattended cars or public areas. Anti-virus software must be installed on mobile devices. Security measures required by IT Security must also be in place when mobile devices utilize wireless transmission of ePHI and confidential information. **Contact the UAMS Technical Support Department at 686-8555 for assistance in securing mobile devices.**

For further information, the U.S. Department of Health and Human Services has published a bulletin on mobile device security.

<http://hipaa.uams.edu/SecurityGuidanceforRemoteUseFinal.pdf>

QUIZ

- 1.) If my supervisor wants my password, I should give it to her.
 - A. True
 - B. False

- 2.) Of the following, which is not a mobile device?
 - A. Laptop Computer
 - B. A telephone connected to a phone jack
 - C. Blackberry
 - D. Mobile Phone

- 3.) Which of the following is an effective password?
 - A. My pet's name
 - B. Xc#g5
 - C. joke1&M
 - D. My last name spelled backwards

Name _____ Dept. _____

Phone number _____

Send to UAMS HIPAA Office, #829, to register for a prize drawing by 2/14/07!!!!!!

Do you have any suggestions or questions you would like to ask? Email us at HIPAA@UAMS.EDU