

UAMS

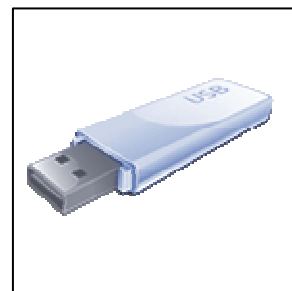
**"Confidentiality is everyone's job,
not everyone's business."**

HIPAA Office, August 15, 2007

DID YOU KNOW...?

Members of the UAMS workforce who use mobile devices to access or record confidential information and protected health information (PHI) are responsible for keeping the information secure. Mobile Devices are defined as Personal Digital Assistants (PDAs), Blackberries, tablet PC's, cellular phones, thumb drives, disk media, text pagers, laptop computers, and any other types of mobile devices or media that receive, record or store information and data. The following are precautions workforce members can take to prevent from loss, theft or unauthorized disclosure from mobile devices.

- Don't store confidential information on the laptop, a CD or a USB thumb drive. Instead, save the data to a UAMS server (use VPN "virtual private networking" to log into work and remotely access the data.) Instructions for VPN set up are located at <http://intranet.uams.edu/it/helpdesk/RemoteAccess.asp> or call the Technical Support Center (686-8555) for assistance.
- If you MUST store any confidential information on portable media (laptop hard drive, CD or thumb drive), encrypt it. This is UAMS policy and you may contact the Technical Support Center (686-8555) for suggestions on encryption.



Physical Security -

- Mobile Devices should NOT be left in a vehicle, but if you must then lock the vehicle and place the device out of sight (under clothes or papers on the floor - the trunk is not a good place.)
- Place your laptop between your feet rather than at the side of your chair while in a public place.
- Make sure your laptop requires a logon / password (14+ characters with a combination of numbers, upper and lower case letters, and special characters.) Password protect your PDA and Blackberry.
- Remember, you are responsible for making sure the data on your portable electronic device is secure. Even if a stolen portable electronic device is recovered and returned in perfect working order, the security of the data on it may still have been compromised. Always report immediately the loss or theft of a device containing sensitive information - even if it was only out of your control for a short time - to the UAMS or ACH IT Department.
- For further information, please refer to UAMS policies [3.1.17 \(Mobile Device Safeguards\)](#), [7.3.14 \(Access Controls for Confidential Information\)](#) and [3.1.38 \(Safeguarding Protected Health Information\)](#). You can also call the technical support center (686-8555) or the IT security office.

Is there a topic you'd like to see covered? Email us at HIPAA@UAMS.EDU. Questions? Call the HIPAA Office at (501) 603-1379.