

UAMS Laptop Security Awareness

Laptops and other portable devices, such as Blackberries, thumb drives and even cell phones, have become an invaluable resource to individuals and companies worldwide. Their portable nature allows greater efficiency and productivity. However, this portable nature also leads to the serious and rising problem of laptop theft, which in turn causes potential data breaches affecting our employees, patients, and finances.

UAMS has been a victim in the past, making it essential that all laptop users take a closer look at the basic security practices surrounding the use of their laptops (or other mobile devices). The goal of this article is to increase the awareness and knowledge of laptop users regarding the steps that can be taken to protect you and the employees, students, and patients at UAMS from the results of laptop theft.

Following some simple guidelines can help us protect our confidential data, including patient health information. First and foremost, ask yourself whether confidential information should be stored on a mobile device. If you can do your job without storing sensitive data on a mobile device, then don't do it! Also, it is much more secure to do your work on the laptop and save the data to a server located behind Enterprise firewalls, using VPN (virtual private networking) to log into work and access the data when necessary. This also protects the data by eliminating the risk of losing it if the hard drive in the laptop failed or became corrupted. If you determine that you must store confidential information on a mobile device, you *must* encrypt it (think of the data being scrambled using a strong password or key). To encrypt a mobile device, the IT stockroom has inexpensive software, called Guardian Edge, available for purchase. Once the software has been purchased, the IT help desk will assist you with installation.

Another basic step is to make sure that the device requires a logon and password. The password would be most secure if it is 14 characters or more with a combination of numbers, upper and lower case letters, and special characters. As always, never share your password with anyone, and don't write it down where someone might find it.

Physical security is another aspect of keeping data secure. Simple steps like keeping the laptop out of sight when left in a vehicle (under clothes or papers in the floor is best; the trunk is not a good place) or between your feet rather than the side of your chair while in a public place can greatly reduce the possibility of it being stolen. Don't store your mobile devices in your vehicle longer than necessary. There are also devices that have been developed to discourage and reduce the risk of laptop theft including alarms, laptop locks, and STOP security plates (these attach to the surface of the laptop leaving a permanent stamp when removed).

The UAMS IT Department and the HIPAA Office are committed to helping you keep our confidential information secure. Please call us if you have any questions or concerns!

<p>UAMS HIPAA Office http://hipaa.uams.edu 603-1379 IT Tech Support 686-8555</p>
--