SECURING LAPTOP COMPUTERS AND FLASH DRIVES

This newsletter is one in a series that provides general information on key components of the HIPAA Privacy and Security Regulations. More detailed information and policies are available on the MCW HIPAA website. In this newsletter we’ll cover how to secure laptop computers and flash drives.

The protection of computer information is critical not only to comply with HIPAA, but for overall security of College information. For example in the case of protected health information, losing control of such data can mean compromising patient information resulting in violation of HIPAA or adversely affecting the reputation of the College. You must adequately protect information for which you are entrusted.

**Laptops**
The following are suggested actions the user should perform to secure their laptop from theft and unauthorized access.

- When leaving a laptop computer unattended, users should apply the “Lock Workstation” feature (ctrl/alt/delete).
- Unattended laptop computers are required to be secured from viewing by password protected screen savers and set to activate the automatic screensaver feature after a period of non-use. The period of non-use shall be for no more than 20 minutes.
- Laptop computers should store confidential and sensitive information on a networked drive and not the user’s laptop hard drive.
- Laptop computers should have firewall software installed.
- Laptop computers should have current antivirus software installed.
- Laptop computers actively connected to the network or information systems should not be left unattended.
- Users must avoid leaving their laptop unattended and should keep laptop computers out of sight when not in use. Laptops that will not be used for several days or longer should be locked out of sight in a secure cabinet or drawer.
- Users should consider using a laptop cable kit to prevent laptop theft by securing your laptop or notebook to your desk.

**Flash Drives**
Flash drives are compact and easy-to-use devices that are similar in use to your computer hard drive. These devices present two primary threats to the network: the introduction of malicious software and data theft/loss. By downloading information from the College network and storing it to a flash drive, there are no longer network controls available to protect the data. College employees and affiliates who utilize flash drives containing Electronic Patient Health Information (EPHI) are responsible for the subsequent use of such items and must take all appropriate and reasonable actions to protect them against damage, theft and unauthorized access. However, the best method of ensuring EPHI is secure is to not store EPHI on a flash drive.

Physical security for flash drives is even more important than for laptops because the flash drives can be slipped into your pocket, carried around your neck or on a keychain for ultimate portable storage. While these ways of transporting the flash drive are convenient for the user, it is also easier for someone to conceal a theft of this device.

Flash drives with password protection and/or encryption software are offered by multiple manufacturers. Many flash drives allow the user to have a public and private partition— the public part is always accessible, while the private part is secured though password or encryption technology. Check with specific manufacturers or your System Manager for security details of specific flash drives. Users can also download encryption software onto USB flash drives from the Internet.

If you believe your laptop or flash drive has been compromised, immediately notify your Supervisor, Public Safety, and your System Manager and/or Information Services.

**COMPUTER SECURITY TIP:**
MCW users on the Collaborative network should log off, but not shut down, their machines at night. MCW-IS ‘pushes’ patch updates overnight and some updates require a reboot to complete the application. Logging off and leaving your machine on allows IS to apply the patches and automatically restart your machine for you.

**YOU CAN REFERENCE ADDITIONAL INFORMATION ON HIPAA PRIVACY AND SECURITY AT:**
The MCW HIPAA website: [http://infoscope.mcw.edu/display/router.asp?docid=7961](http://infoscope.mcw.edu/display/router.asp?docid=7961)