Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #12

Device and Media Controls Procedure

Last Revised: 3/15/2005	*Approved: 12/12/2005*

Scope:

Outline procedures that govern receipt, removal and movement of hardware and electronic media containing EPHI within the workspace of the department. These policies and procedures pertain to the use of hard drives, storage systems, removable disks, floppy drives, CD-ROMS, memory sticks, and all other forms of removable media and storage devices.

Data Destruction of EPHI on Storage Device Prior to Discarding or Reuse of Storage Device:

PC's & Laptops: Before wiping data from any of these types of devices, users, system managers or the OIS staff must insure that there is no EPHI located on the device. If no EPHI is found (at present), the device may be wiped clean using a data destruction tool. If EPHI is found to reside on the device, AND, it is the only copy of said EPHI, that data must be copied to an alternate and equally secure location, prior to the drive or disk being erased. When a PC or laptop is leaving the department for whatever reason, the device must be wiped clean using the data destruction tool prior to leaving the department. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended. Note that in cases where a hard drive is not functioning and a data destruction tool cannot be used, the drive must either be degaussed or physically destroyed.

PDA's: Users, system managers and OIS staff must insure that all EPHI has been removed prior to allowing a PDA to being transferred to another user or prior to being destroyed. This must be accomplished by a hard reset on the device to insure all data has been removed.

CD's, Floppy Disks, etc: If any of these types of media storage are known to contain EPHI, they must be destroyed when no longer needed. Floppy disks must be erased using the data destruction tool, or physically destroyed and CD's must be physically broken prior to disposal.

Flash Memory Sticks: Memory sticks in which EPHI has been stored must be formatted and the data destroyed using the data destruction tool. If a memory stick is no longer working and accessible, and cannot be formatted, it must be physically destroyed prior to disposal.

Storage:

If any of these devices are used for storage of medium or high risk EPHI, the device must adhere to the procedures outlined in #11 Desktop and Wireless Computer System Procedure.

Moving:

PC's and Laptops: The user must oversee the movement of a device containing EPHI if moving is performed by a third party (e.g. moving company) and the device is not otherwise physically secured.

PDA's, Flash Memory Sticks, Floppy Disks, and CD's: Users must use care when carrying these devices from location to location to ensure they are not lost or stolen. Files located on the devices should be either encrypted, or password protected. See Procedure #17 Transmission Security for more information on encrypting files.

Offsite backup media: If removable media used for backup and disaster recovery is stored and transported between locations using a secured environment, the use of a data destruction tool between uses is not necessary.