

TITLE: EPHI7. INFORMATION SECURITY: BACKUP, DEVICE AND MEDIA CONTROLS

POLICY:

CUMC takes reasonable steps to protect, account for, properly store, back up and dispose of its hardware and electronic media in use for Electronic Protected Health Information (EPHI).

PURPOSE:

CUMC secures information stored on disks, tapes, and other electronic media.

APPLICABILITY:

CUMC faculty, staff, students, owners, custodians, and users of EPHI systems

PROCEDURE:

1. Types of hardware and electronic media to which this policy applies include:
 - Computers (desktops, laptops, tablets, other)
 - Personal Digital Assistant (PDA) storage
 - Tapes
 - Hard drives
 - Portable storage media (Compact Disc/ Digital Video Disc/Zip/floppy/ other), memory cards (PC, Compact Flash, Secure Digital, other), memory sticks, Universal Serial Bus storage devices (camera, cell phones, etc.) with ability to store information
2. Workforce members may not attempt to physically duplicate, copy or move EPHI for which they have not been granted proper authorization from Department Chair (or a designee) or a manager at Director level or above. The Owner of an EPHI system may establish additional limits for the original information for the Users and Custodians of the system, which may not be overridden in the User departments. All institutional policies are applicable on any copies that are made, unless the copy is transferred over to a business partner, for which appropriate confidentiality or business associate agreement must exist prior to the transfer. The workforce member who makes the copies is responsible for the security of the information as per institutional policies.
3. If a portable storage media is used to store PHI, it should be stored in a locked area. If the portable storage media is taken out of the hospital premises, the data must be encrypted.

3. All computers connected to institutional networking resource must be registered in institutional asset database managed by CUBHIS or must use institutional authentication methods that identify the owner with a valid authorization to connect to the network to access resources, and create an appropriate audit log. Security practices required on such computers is in **Workstation security and use policy** (#EPHI5).
4. Custodians make exact and retrievable backup copies of EPHI on an ongoing basis to guard against system failures and data corruption. (Also see **Information security: Disaster contingency and recover plan policy** (#EPHI9).) Custodians take reasonable steps to ensure that the EPHI that is backed up in connection with movement of equipment into, out of, and within its facilities can be recovered following a disaster or other emergency, or a failure of the equipment during movement.
5. Owners and custodians may arrange to store backup copies in a secure remote location away from where the EPHI system being backed up is housed. The remote storage is required to have appropriate physical and environmental protection, as well as the ability to retrieve the backup copies as necessary to restore the system by authorized personnel.
6. Owners and custodians take reasonable steps so that before media (tapes, disks, storage cards, etc.) are re-used across different EPHI and other systems, the EPHI on the media is completely and irreversibly removed using erasure tools. For some media (such as CD, tapes, etc.) on which information is stored, may be physically destroyed if the media are to be disposed of permanently. Note that the Environment Health and Safety policy on **Collection and Storage of Computer Monitors, Peripherals, and other Electronic Equipment** should be followed for permanent disposal of the same.

POLICY MAINTENANCE:

Information Security Office

REFERENCES:

All information security policies

CU Administrative policies in Computing & Technology

Health Insurance Portability and Accounting Act of 1996, 45 CFR

164.310(d)(1),

164.310(d)(2)(i), 164.310(d)(2)(ii),

164.310(d)(2)(iii), 164.310(d)(2)(iv)

REVIEW/REVISION DATE:

November 2007