
Department: UW Medicine Information Technology Services

Policy Number: SEC-05.01 – Media Handling Standard

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

This standard sets forth media handling requirements to protect UW Medicine¹ information systems and related items from damage, theft and unauthorized access. This standard applies to information classified as CONFIDENTIAL or RESTRICTED, including information contained on hardware and electronic media stationary or in movement (in and out of a facility as well as between locations within a facility or facilities). This standard supports the UW Medicine Information Security policy, *SEC-05 – Communications and Operations Management Policy*.

Definitions

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms*.

Standards

I. Media Handling Standard for RESTRICTED OR CONFIDENTIAL Information

Device and media controls are required to protect the confidentiality and integrity of electronic media and hardware as information is received into and moved around and out of the facility. Information must be handled consistent with its classification regardless of where it resides, for example: documents, computing systems, mobile computing, mobile communications, mail, voice communications, multimedia, postal services/facilities, and/or use of fax machines and networks.

¹ For the purposes of HIPAA, UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; UW Medicine Eastside Specialty Center; Hall Health Primary Care Center; University of Washington Physicians; as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.

A) **Media Controls**

Media control measures are required in order to ensure physical and environmental protection and accountability for tapes, diskettes, printouts, and other media and to prevent the loss of confidentiality, integrity, or availability of information. This includes data or software that is stored outside the system.

The extent of media control depends upon the type of data, the quantity of media, and the nature of the user environment. Physical and environmental protection must be used to prevent unauthorized individuals from accessing the media and to prevent damage from such factors as heat, cold, or harmful magnetic fields.

B) **Labeling**

Labels may be used to identify media that require special handling or to log media (for example, serial/control numbers or bar codes).

If labeling is used for special handling instructions, appropriate training is required for all individuals who handle the media.

C) **Accounting for Movement of Hardware and Electronic Media**

A log must be kept to record the movements of hardware and electronic media and to document the persons accountable for the hardware. Logging of media also supports accountability by holding individuals responsible for how they handle media. Logs may include control numbers (or other tracking data), times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits must be conducted to determine if any items have been lost and to ensure that items are in the custody of the individuals named in control logs.

Before moving equipment that contains electronic Protected Health Information (ePHI), the System Operator must determine if backup copies exist. If not, backups must be made prior to moving equipment.

D) **Physical Access Protection**

Physical access controls are required to limit problems like lost, stolen, destroyed media. Physical access controls include locked doors, desks, file cabinets, or safes.

If the information is classified as CONFIDENTIAL, the output from the media should be sent to a secure location (e.g., printing to a printer in a locked room instead of to a general purpose printer in a common area).

Physical protection is extended to backup copies stored offsite. Offsite backup copies are provided an equivalent level of protection to media stored onsite. (Equivalent does not mean that the

measures need to be exactly the same. Off-site location controls are likely to be different from onsite controls.)

E) **Environmental Protection**

Media has different sensitivities to environmental factors. Magnetic media, such as diskettes or magnetic tape must be protected from heat, liquids, magnetism, smoke, and dust.

F) **Retention**

Records are to be retained according to University of Washington and state retention policies.

University of Washington General Records Retention Schedule:
<http://www.washington.edu/admin/recmgt/retention.schedule.html>

Agencies of Washington State Government; General Records Retention Schedules:
<http://www.secstate.wa.gov/archives/pdf/STATE%20GS%20MANUAL%204-2002.pdf>

UW Records Management Services can be used for storage of media:

<http://www.washington.edu/admin/recmgt/office/index.html>

Note: Records with a CONFIDENTIAL data classification (example – protected health information) must be maintained in a secure location with controlled access.

II. **Disposal of Media**

Protected health information, proprietary information, and other confidential information may be stored on a variety of media. RESTRICTED and/or CONFIDENTIAL information shall not be disposed of as general waste.

The workforce member tasked with disposing of the media must ensure that information is not improperly disclosed. This applies both to media that is *external* to a computer system, such as a diskette, and to media *inside* a computer system, such as a hard drive.

A) All media that has RESTRICTED and/or CONFIDENTIAL information must be disposed of securely and safely when no longer required.

- UW Medicine has established the following procedures for the secure disposal of media:
- Paper Documentation
Paper records shall be shredded, pulped or otherwise obliterated in a manner that prevents reconstruction.

- Microfilm/Microfiche
Microfilm and microfiche must be pulverized.
- Laser Disks
The laser disks used in write once-read many (WORM) document imaging applications shall be pulverized.
- Floppy Disks
Floppy disks shall be pulverized.
- Compact Discs (CDs) and Digital Versatile Disc (DVDs)
CDs/DVDs shall be pulverized.
- Magnetic Tape & Video Tape
The preferred method for destroying computerized data is magnetic degaussing. If destruction is not achieved by degaussing, destruction must be executed in a manner that assures the information cannot be reconstructed.
- USB Drive, PDA, Cell Phones, and other mini drives
Users must follow the manufacturer's guidelines for proper cleaning and removal of all data on the device.
- Hard Drives
Multi-pass binary overwrite software appropriate to the system is to be selected by the System Operator.

Recommended tools for compliance with this standard can be found at: <http://security.uwmedicine.org/resources/default.asp>

- Carbon Rolls (from printers or fax machines)
Send carbon rollers that have been removed from printers or fax machines to Environmental Services for destruction by autoclaving.
- B) If media containing restricted or confidential information is to be provided outside UW Medicine, the workforce member must ensure that an appropriate contractual agreement is in place for the disposal of the media. For more information, see UW Medicine Privacy Policy, *PP-12 Use & Disclosure of Protected Health Information by Business Associates*.

III. **Media Re-use**

For electronic media intended for reuse System Operator must ensure proper methods and controls are used. System Operator or designee shall log re-use of hard drives in order to maintain an audit trail.

All electronic media intended for reuse must be processed in one of the following two ways:

1. *Overwrite*. Multi-pass binary overwrite software appropriate to the system is to be selected by the System Operator.

2. *Degauss*. Degaussing magnetically erases data from magnetic media. Two types of degausser exist: strong permanent magnets and electric degaussers.

References:

- I.** 45 CFR Part 164; Section 164.310(d)(1) Device and Media Controls; (2) (i) Disposal, (ii) Media Re-use, (iii) Accountability, (iv) Data Backup and Storage
- II.** 45 CFR Part 164; Section 164.312 (c) (1) Integrity
- III.** 45 CFR Part 164; Section 164.312 (e) (2) (i) Integrity Controls
- IV.** International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 8, Communications And Operations Management
- V.** Chapter 40.14 RCW
- VI.** RCW 18.51.300 Retention and preservation of patient records.
- VII.** RCW 19.215 - Disposal of personal information
- VIII.** UW Records Management Services:
<http://www.washington.edu/admin/recmgt/office/index.html>

UW Medicine IT Services: _____ Date: _____

James S. Fine, M.D., CIO, ISO
