



[Home](#) | [Message Board](#) | [Educational/Training Programs](#) | [Policies & Procedures](#) | [UP&S Employee Handboo](#)

HIPAA Security Policies

Workstation and Storage Media Hardware Disposal and Re-Use

**DRAFT adopted by HIPAA Security Committee on 1/20/04
REVISED 3/24/04 and 10/25/04, REVISIONS ADOPTED 11/1/04**

Policy Summary

This policy governs the procedures required prior to the disposal or re-use of any workstation or storage media hardware from or within the Marshall University Joan C. Edwards School of Medicine / University Physicians & Surgeons (SOM/UP&S).

Purpose

This policy reflects the commitment to ensure that all workstation and storage media hardware disposed of or re-used by SOM/UP&S is free of electronic protected health information (PHI) and other confidential data or information.

Policy

1. Local, direct attached storage (DAS), such as workstation hard drives, or removable media -- including but not limited to floppy disks, ZIP disks, rewriteable optical disks (CD/DVD) and non-volatile memory (USB memory keys, secure digital cards, etc.) -- is not to be used for the enduring storage of electronic PHI. All appropriate and relevant information should be entered into a patient's medical record at the earliest opportunity.
2. A SOM/UP&S workforce member who generates, transcribes or records electronic PHI on local or removable media is solely responsible to safeguard the confidentiality and ensure the integrity of that electronic PHI until such time as it is entered into the patient's medical record.
3. SOM/UP&S will not be responsible for creating or maintaining backups of any electronic PHI that is not part of the organization's official medical record system.
4. Any local, direct attached storage (DAS) or removable media that is used to store electronic PHI should not be transferred or provided to another user, disposed of or transferred or released outside of SOM/UP&S for any reason (such as for vendor or manufacturer service, maintenance, repair or replacement of the device or the host workstation or server) until it has been cleaned of any PHI or other confidential data or information by means of the procedures here described.
5. Any workstation or storage media owned by a department or division of SOM/UP&S must be disposed of in accordance with any applicable federal, state, local and university laws and regulations regarding the surplus of institutionally-owned equipment.
6. It is the responsibility of the chair or head of the department or division owning the workstation or local storage media to ensure that this policy is adhered to for any devices disposed of or re-used. For removable media, it is the responsibility of the end-user who uses that media to store electronic PHI or other confidential data to ensure that this policy is adhered to for any devices disposed of or re-used.

Scope / Applicability

This policy applies to all workstation and storage media hardware purchased, owned, controlled or used by SOM/UP&S, including equipment purchased by the Marshall University Research Corporation on behalf of individuals or departments within SOM/UP&S, equipment donated and equipment in any other way obtained and owned by SOM/UP&S. Chairs and heads of departments or divisions having ownership of such equipment are

responsible for providing access to the workstations or storage media for processing prior to their disposal.

Regulatory Categories

Physical Safeguards

Regulatory Type

REQUIRED implementation specification for workstation disposal.

REQUIRED implementation specification for media re-use.

ADDRESSABLE implementation specification for accountability.

ADDRESSABLE implementation specification for data backup and storage.

Regulatory References

1. §164.310(d)(2)(i) "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."
2. §164.310(d)(2)(ii) "Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."
3. §164.310(d)(2)(iii) "Maintain a record of the movements of hardware and electronic media and any person responsible therefore."
4. §164.310(d)(2)(iv) "Create a retrievable, exact copy of electronic protected health information, when needed, before the movement of equipment."

Definitions

Workstation

"An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment" (§164.304).

Responsible Department

The chair or head of the department or division having ownership of such equipment is responsible for providing access to the workstations or storage media for processing prior to their disposal.

Related Policies

- [Marshall University Purchasing Handbook](#)
- [Marshall University Information Security Policy](#)

Renewal / Review

This policy shall be reviewed annually to determine if it complies with current HIPAA Security regulations and is appropriate given current technology. In the event that significant related regulatory changes occur, the policy will be reviewed and updated as needed.

Procedures

Re-Use of Workstations or Local Direct Attached Storage (DAS) Media:

1. At least one week prior to the transfer of any workstation or local storage media from one user to another within SOM/UP&S, the department or division having ownership will provide the device to the Division of Information Technology & Medical Informatics (DITMI).

2. DITMI will wipe the workstation or storage media's data contents with a utility that meets Department of Defense cleaning and sanitizing standard DoD 5220.22-M.
3. DITMI will reinstall a default operating system and software image consisting of appropriately licensed client software, such as the operating system, an office automation suite and anti-virus software.
4. DITMI will document the following information about the process: workstation make, model, serial number and Marshall University inventory tag number; owning department or division; DITMI technician performing the process; and date of completion.
5. The department or division owning the workstation or local storage media will document the following information about the process: user from whom the device is being transferred; user receiving the device; and date of transfer completion.

Transfer or Release of Workstations or Local Direct Attached Storage (DAS) Media for other than Disposal:

1. Workforce members must take steps to prevent the inappropriate disclosure of EPHI as a result of the transfer or release of workstations or local direct attached storage (DAS) outside of SOM/UP&S for reasons other than disposal (for example: the transfer of a workstation or DAS to a vendor or manufacturer for service, maintenance, repair or replacement).
2. DITMI will provide a hard drive eraser (degausser) which can be used to wipe the contents of DAS device prior to their transfer or release outside of SOM/UP&S.
3. DITMI will document the following information about the process: workstation or DAS device make, model, serial number and Marshall University inventory tag number; owning department or division; DITMI technician performing the process; and date of completion.

Disposal of Workstations or Local Direct Attached Storage (DAS) Media:

1. At least one week prior to the disposal of any workstation or storage media hardware, the department or division having ownership will provide the device to the Division of Information Technology & Medical Informatics (DITMI).
2. DITMI will wipe the workstation or storage media's data contents with a utility that meets Department of Defense cleaning and sanitizing standard DoD 5220.22-M.
3. DITMI will document the following information about the process: workstation make, model, serial number and Marshall University inventory tag number; owning department or division; DITMI technician performing the process; and date of completion.
4. DITMI will not attempt to reinstall any software onto the workstation or storage media.
5. The owning department or division is responsible for providing any desired, original installation media for appropriately licensed software and for disbursing the machine along the next step in the disposal process following the completion of the steps here described.

Re-Use and Disposal of Removable Media:

1. Removable media used to store electronic PHI or any other confidential information should never be transferred to or used by anyone other than the proper recipient of that specific electronic PHI or confidential information.
2. Removable media used to store electronic PHI or any other confidential information must be disposed of in such a way that it can never be used again for the retrieval or storage of data. DITMI will make available a disk shredder device for the destruction of such removable media, but it remains the responsibility of the individual end-user of the removable media to ensure that any electronic PHI on it is properly safeguarded.

Adoption

Adopted by **SOM/UP&S Board of Directors** on [date].

Copyright © 2003 University Physicians & Surgeons - All Rights Reserved | Last Modified March 24, 2003