

**1.0 Purpose**

These procedures address the HIPAA Security Standard *164.310(d)(1) Device and Media Controls*: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

**2.0 Definitions**

**2.1 Degauss:** To demagnetize. Degaussing a magnetic storage medium such as a hard disk removes all stored data. A *degausser* is a device used for this purpose.

**2.2 Workforce:** All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

**3.0 Procedures**

**3.1 Evaluate methods for final disposal of electronic protected health information (ePHI)** by determining and documenting the appropriate methods to dispose of hardware, software, and the data itself; and assuring that ePHI is properly destroyed and cannot be recreated.

**3.2 Develop and implement procedures for the re-use of electronic media by ensuring that ePHI previously stored on electronic media cannot be accessed and reused** by identifying removable devices and their use; and by ensuring that ePHI is removed from reusable media before it is used to record new information.

**3.3 Maintain records of hardware, media, and personnel** by ensuring that ePHI is not inadvertently released or shared with any unauthorized person; and by ensuring that an individual is responsible for, and records the receipt and removal of hardware and software containing ePHI.

**3.4 Develop backup procedures to ensure that the integrity of ePHI will not be jeopardized during equipment relocation** by ensuring that an exact, retrievable copy of the data is retained and protected.

**3.5 Securely sanitize or destroy** all media that contains restricted or confidential information before disposing of equipment:

**3.5.1 Sanitization or Destruction of Devices Supported and Maintained by School of Nursing IT:** For devices that are supported and maintained by School of Nursing IT, contact the

SON IT Help Line at (415) 502-8286.

### **3.5.2 Sanitization or Destruction of Devices not Supported or Maintained by School of Nursing IT:**

**3.5.2.1 Sanitize Hard Disk:** The hard disk must be crushed, drilled, degaussed, or incinerated.

**3.5.2.2 Portable media:** Destroy floppy disks, tapes and CD-ROM disks by crushing, incinerating, shredding, or melting.

**3.5.2.3 If Unable To Perform Sanitization Or Destruction:** Contact the IT Customer Support Center at (415) 514-4100 to request services from an authorized service provider.

**3.6 Media Re-use:** Implement procedures to securely sanitize media before transferring or donating any equipment that is owned by the UCSF School of Nursing.

**3.6.1 Determine sanitization method:** Three techniques approved by the US Department of Defense (DoD) standard 5220.22-M are commonly used for media sanitization: *overwriting, degaussing, and physical destruction.*

**3.6.2 Overwriting:** Overwriting is an effective method for clearing data from magnetic media. Overwriting is the only DoD-approved sanitization method that consistently does not render the device unusable in situations where media is to be redeployed.

As the name implies, overwriting uses a program to write (1s, 0s, or a combination) onto the media. Common practice is to overwrite the media three times. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a delete command is used).

Overwriting requires that the media be in working order. When selecting software to perform overwriting, make sure that it meets DoD standard 5220.22-M.

### **3.6.3 Sanitization of Hard Disk**

**3.6.3.1** Obtain DoD standard 5220.22-M-compliant overwriting software.

**3.6.3.2** Remove all boot-up and BIOS passwords.

**3.6.3.3** Run the executable utility as instructed by software documentation.

**3.6.3.4** Reformat the hard disk and install a new operating system to ensure that the disk is re-useable.

### **3.6.4 Sanitization of other media**

**3.6.4.1** If there is any risk of disclosure of sensitive data on media other than computer hard drives, employ the appropriate sanitization methods as outlined in the Recommended DoD Clearing and Sanitization Matrix displayed in this section.

Memory components should also be sanitized before being disposed or released. Memory components reside on boards, modules, and sub-assemblies. A board can be a module or it may consist of several modules and sub-assemblies. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release. Memory components are categorized as either volatile or nonvolatile, as described below:

- Volatile memory components *do not* retain data after removal of all electrical power sources; and when re-inserted into a similarly configured system, volatile memory components do not contain residual data, i.e. SRAM, DRAM.
- Nonvolatile memory components *do* retain data when all power sources are discontinued. Nonvolatile memory components include Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM) and their variants.
- Memory components that have been programmed at the vendor's commercial manufacturing facility and are considered unalterable in the field may be released. Otherwise, DoD Sanitization Procedures must be followed.

### **US Department of Defense 5220.22-M Clearing and Sanitization Matrix**

Media	Clear	Sanitize
<b>Magnetic Tape</b>		
Type I*	a or b	a, b, or m
Type II**	a or b	b or m
Type III***	a or b	M
<b>Magnetic Disk</b>		
Bernoullis	a, b, or c	M
Floppies	a, b, or c	M
Non-Removable Rigid Disk	c	a, b, d, or m
Removable Rigid Disk	a, b, or c	a, b, d, or m
<b>Optical Disk</b>		
Read Many, Write Many	c	M
Read Only		M, n
Write Once, Read Many (Worm)		M, n
<b>Memory</b>		
Dynamic Random Access memory (DRAM)	c or g	c, g, or m
Electronically Alterable PROM (EAPROM)	I	j or m

Electronically Erasable PROM (EEPROM)	I	h or m
Erasable Programmable ROM (EPROM)	k	l, then c, or m
Flash EPROM (FEPRM)	I	c then I, or m
Programmable ROM (PROM)	c	M
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	M
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m
Read Only Memory ROM		M
Static Random Access Memory (SRAM)	c or g	c and f, g, or m
<b>Equipment</b>		
Cathode Ray Tube (CRT)	g	Q
<b>Printers</b>		

Impact	g	p then g
Laser	g	o then g

**\*Type 1 magnetic tape** includes all tapes with a coercivity factor (amount of electrical force required to reduce the recorded magnetic strength to zero) not exceeding 350 oersteds.

**\*\*Type 2 magnetic tape** includes all tapes with a coercivity factor between 350 and 750 oersteds.

**\*\*\*Type 3 magnetic tape** commonly referred to as high-energy tape (4 or 8mm tape are examples), includes all tapes with a coercivity factor between 750 and 1700.

### Sanitization Procedure Key

- a. Degauss with a Type I degausser. (John, please provide a definition of Type I degausser)
- b. Degauss with a Type II degausser. (John, please provide a definition of Type II degausser)
- c. Overwrite all addressable locations with a single character.
- d. Overwrite all addressable locations with a character, its complement, then a random character and verify. *THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS EXTREMELY CONFIDENTIAL OR SENSITIVE INFORMATION.*
- e. Overwrite all addressable locations with a character, its complement, and then a random character.
- f. Each overwrite must reside in memory for a period longer than the classified data resided.
- g. Remove all power to include battery power.
- h. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
- i. Perform a full chip erase as per manufacturer's data sheets.
- j. Perform step I, then step c, three times.

- k. Perform an ultraviolet erase according to manufacturer's recommendation.
- l. Perform step k, but increase time by a factor of three.
- m. Destroy – disintegrate, incinerate, pulverize, shred, or melt.
- n. Destruction required only if classified information is contained.
- o. Run five pages of unclassified text (font test acceptable).
- p. Ribbons must be destroyed. Platens must be cleaned.
- q. Inspect and/or test screen surface for evidence of burned-in information. If present, the cathode ray tube must be destroyed.

*The preceding information was extracted from the US Department of Defense 5220.22-M Clearing and Sanitization Matrix.*

**3.7 Data Backup and Storage Prior to Relocation:** Implement procedures in order to ensure adequate data backup and storage before relocation of equipment:

**3.7.1** Before relocating any computer hardware equipment, the appropriate workforce member must backup and store designated data.

Backups will be accomplished via duplication of application files contained on disk storage systems and transfer to removable magnetic tape media. Appropriate IT applications groups must be consulted to determine which applications and files should be backed up.

**3.7.2** Tapes will be delivered to the tape librarian.

**3.7.3** The data center tape librarian is responsible for packaging tapes for vendor pickup.

**3.7.4** Define schedule and frequency that tapes are picked up by an outside vendor.

**3.7.5** Define personnel authorized to retrieve a tape must first phone the outside storage vendor.

**3.7.6** Follow Recovery procedures as defined by appropriate IT support group

- Technical support staff for operating system and utilities software

- Applications support staff for application data.
- Computer operations department will work with staff to restore data when necessary.

**3.8 Device and Media Accountability:** Implement procedures to address the accountability of all media that contains restricted or confidential information:

**3.8.1 Maintain records of movements of hardware or electronic media:** The department that manages and supports the hardware or electronic media that is to be moved is responsible for maintaining records that should include:

- Description of hardware and/or electronic media item
- Name of person or department requesting the move of the hardware and/or electronic media
- Date and time of move
- Scheduled return date
- Date and time hardware and/or electronic media was returned
- Name and signature of person authorizing the move
- Name and signature of person authorized to receive the moved item (s)
- Name and signature of person returning the item (s)
- Name and signature of person authorizing the return
- Name and signature of person returning the item (s)

**4.0 Initiation and  
Control Reporting**

**5.0 Records &  
Documentation  
Control**

**6.0 Related  
Documents**

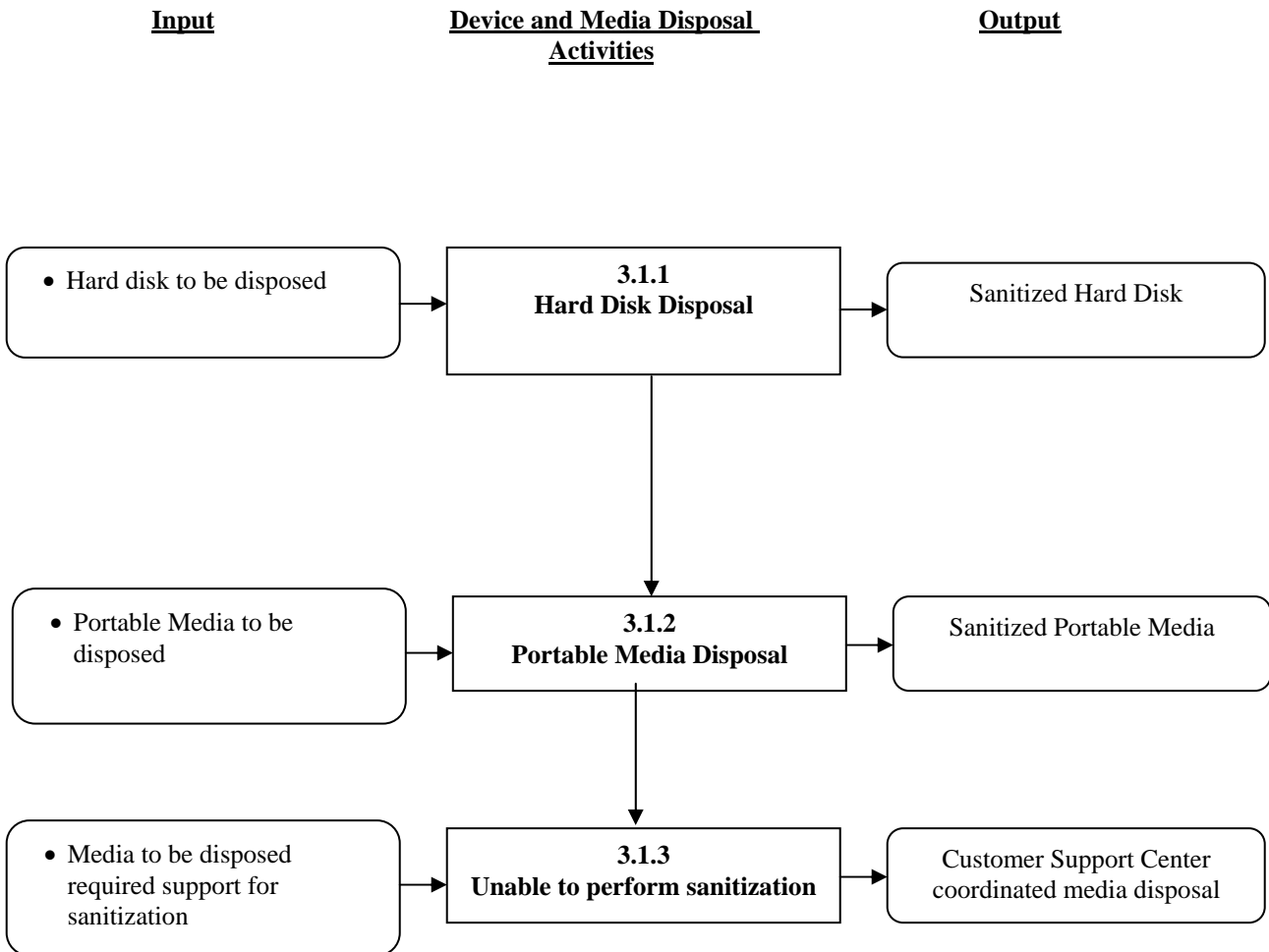
Document Name	Procedure No.
---------------	---------------

HIPAA Security Rules: Device and Media Controls	<b>164.310(d)(1)</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Special Publication: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule – National Institute of Standards and Technology (NIST)	<b>SP 800-66</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
University of California Business and Finance Bulletin IS-3 Electronic Information Security	<b>BFB IS-3</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a> or <a href="http://www.ucop.edu/ucophome/policies/bfb/is3.pdf">http://www.ucop.edu/ucophome/policies/bfb/is3.pdf</a>
UCSF Information Security and Confidentiality Policy	<b>650-XX</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Information Security and Confidentiality Policy	<b>5.01.04</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Facility Access Controls Procedures	<b>60.008</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>

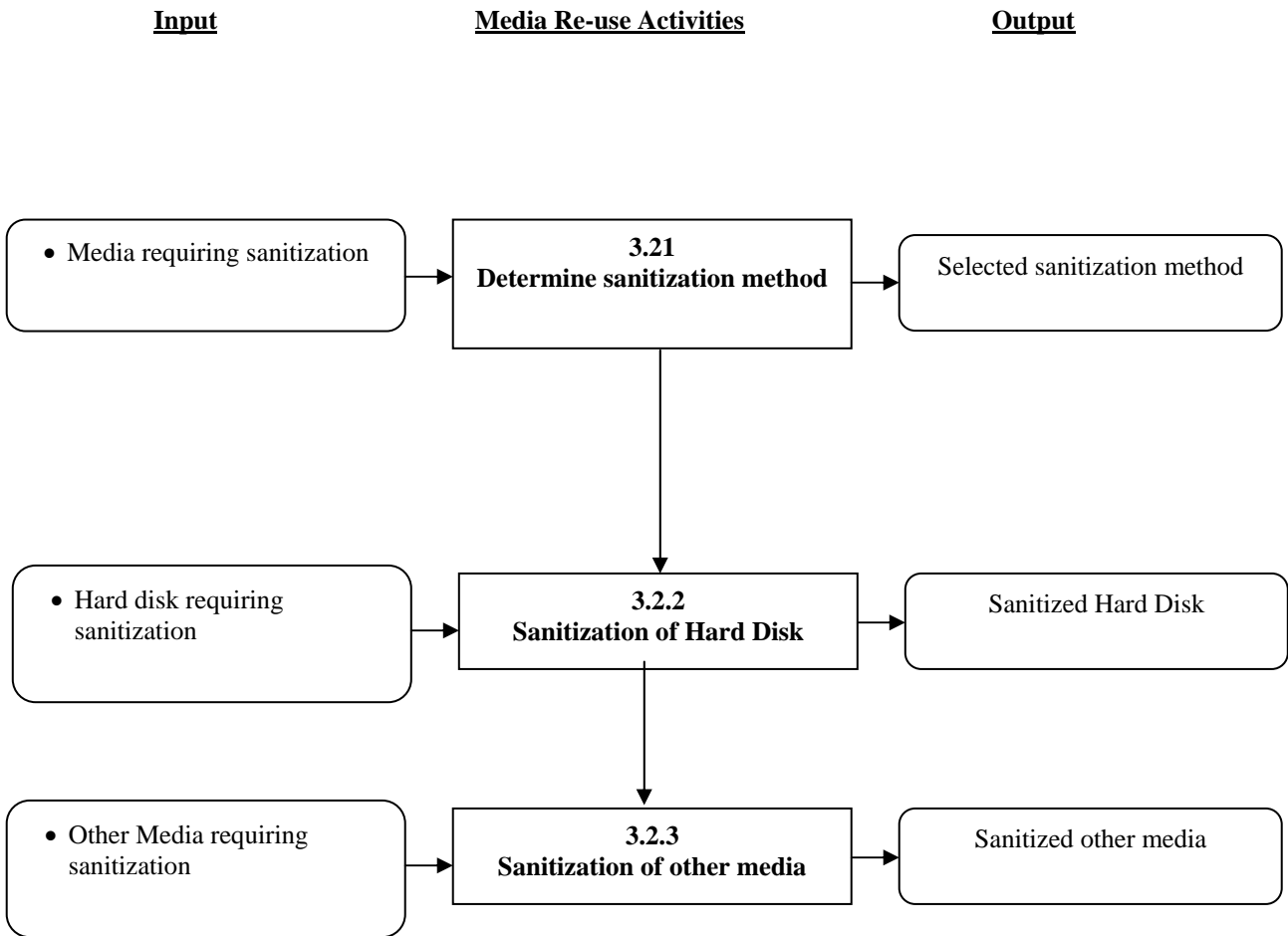
### REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A		Ellen Amsel, Robert Descoteaux, and Todd Lawrence with SOM Physician Resident	Initial Release
B	11/27/06	Rob Slaughter	Adapted for School of Nursing

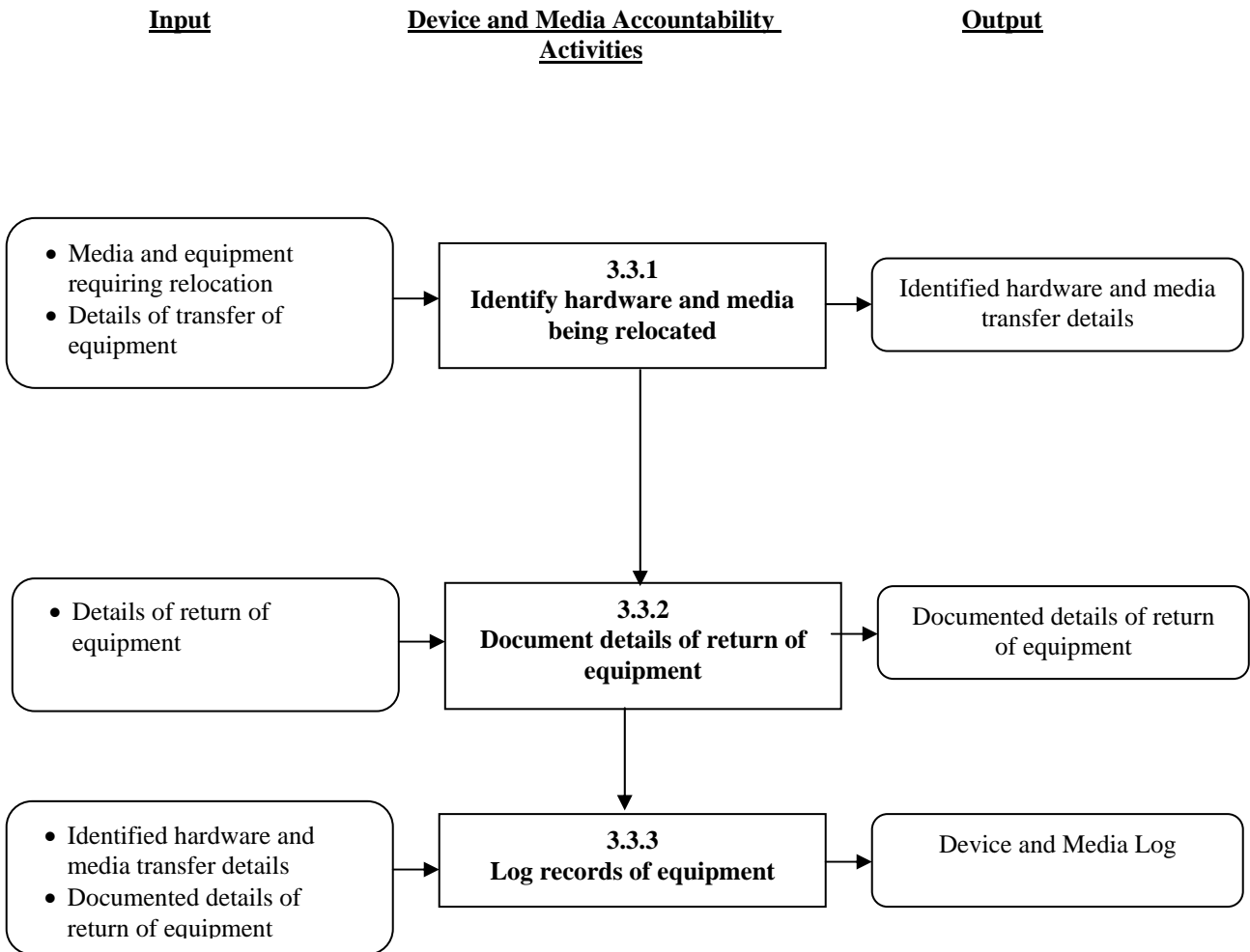
**Appendix A: Device and Media Disposal Process Flow**



**Appendix B: Media Re-use Process Flow**



**Appendix C: Device and Media Accountability Process Flow**



**Appendix D: Data Backup and Storage Prior to Relocation Process Flow**

