



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

OCT 10 2008

MEMORANDUM FOR: TRICARE MANAGEMENT ACTIVITY
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL
INFORMATION SYSTEMS OFFICE
TRICARE REGIONAL OFFICE – NORTH
TRICARE REGIONAL OFFICE – SOUTH
TRICARE REGIONAL OFFICE – WEST

SUBJECT: Military Health System (MHS) Information Assurance (IA) Policy Guidance
and MHS IA Implementation Guides

In accordance with Assistant Secretary of Defense (Health Affairs) (ASD (HA)) memorandum, "Military Health System (MHS) Information Assurance (IA) Implementation Guides," dated July 19, 2005, this office has completed a review of the MHS IA Implementation Guides. As a result, the following documents have been updated:

- Implementation Guide No. 1, "Governance"
- Implementation Guide No. 2, "Sanitization"
- Implementation Guide No. 3, "Incident Reporting"
- Implementation Guide No. 4, "Employee Behavior"
- Implementation Guide No. 7, "Data Integrity"
- Implementation Guide No. 9, "Configuration Management"
- Implementation Guide No. 10, "System Life Cycle Management"
- Implementation Guide No. 11, "Public Key Infrastructure (PKI) and PK Enabling"
- Implementation Guide No. 12, "IAVM Program"
- Implementation Guide No. 13, "IA Training, Education and Awareness"
- Implementation Guide No. 14, "INFOCON"

The MHS IA Implementation Guides were developed in collaboration with the MHS IA Working Group, and staffed, coordinated, and approved by the Enterprise Architecture Board.

The provisions of the MHS IA Implementation Guides are policy for all TRICARE Management Activity (TMA) Directorates, TRICARE Regional Offices (TROs), and the Joint Medical Information Systems (JMIS) Office.

For TRICARE Contractors, these documents are policy if required by contract; otherwise, they serve as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate these documents into their information assurance policies and procedures.

For additional information, please contact Ms. Dorothy S. Williams, Chief, MHS IA Program at (703) 681-7735 or via e-mail at dorothy.williams@tma.osd.mil.



Charles M. Campbell
Chief Information Officer
Military Health System

Attachments:

As stated

cc:

Deputy Surgeon General of the Army
Deputy Surgeon General of the Navy
Deputy Surgeon General of the Air Force

| | | |
|--|--|--------------------------------------|
|  <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS) INFORMATION ASSURANCE (IA) IMPLEMENTATION GUIDE</p> | IMPLEMENTATION GUIDE No. 2 | |
| | EFFECTIVE DATE 07/19/05 | REVISED DATE 10/10/08 |
| <p>Subject: SANITIZATION AND DISPOSAL OF ELECTRONIC STORAGE MEDIA AND MHS INFORMATION TECHNOLOGY EQUIPMENT PROCEDURES</p> | | |

1. PURPOSE AND SCOPE

1.1. The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures.

1.2. The MHS procedures for sanitization and disposal of electronic storage media and information technology (IT) equipment ensure the appropriate actions are executed when disposing of IT equipment and electronic storage media containing DoD Sensitive Information (SI) as defined in DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003. Personally Identifiable Information (PII) and Personal Health Information (PHI) are DoD SI.

1.3. This implementation guide provides TMA Component personnel and contractors with specific guidance and procedures to ensure disposition and sanitization of MHS IT equipment and electronic storage media is executed accordingly prior to transfer within MHS or permanent removal from the MHS and DoD custody.

2. POLICY

2.1. It is MHS policy that:

2.1.1. All TMA Components shall sanitize IT equipment and electronic storage media prior to disposal in accordance with DoD 5200.1-R, "Information Security Program," January 1997 and Assistant Secretary of Defense, Command, Control, Communications and Intelligence (ASD C3I) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001.

2.1.1.1. The Information Owner is responsible for establishing appropriate controls for disposal in accordance with DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003 (paragraph E2.1.33).

2.1.1.2. TMA Components shall utilize the “Record of IT Equipment Sanitization” form (pages 9-10) as the sanitization and clearing label, for **ALL** dispositions of electronic storage media and MHS IT equipment. The signed “Record of IT Equipment Sanitization” label shall be affixed to the electronic storage media, computer housing, or appropriate surface.

2.1.1.3. The TMA Privacy Office shall retain disposition of electronic storage media and MHS IT equipment records for a minimum of six years to meet Health Insurance Portability and Accountability Act (HIPAA) requirements and to strengthen the MHS security posture.

2.1.1.4. Certified overwritten electronic storage media shall be verified on a random basis by two trained individuals other than the person who performed the overwrite process. No fewer than 20% of all overwritten electronic storage media shall be examined in one verification process.

3. PROCEDURES

3.1. Sanitization must be performed on electronic storage media and IT equipment to ensure that information is removed from the electronic storage media in a matter that gives assurance that the information cannot be recovered. Before the sanitization process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

3.2. There are three acceptable DoD methods to be used for the sanitization of electronic storage media and IT equipment:

3.2.1. Overwriting

3.2.2. Degaussing

3.2.3. Physical Destruction

3.3. The method used for sanitization depends upon the operability of the electronic storage media and IT equipment:

3.3.1. Operable electronic storage media and IT equipment that shall be reused must be overwritten prior to disposition. If the operable electronic storage media and IT equipment is to be removed from service completely, it must be physically destroyed or degaussed.

3.3.2. If the electronic storage media and IT equipment is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

3.4. Clearing data (deleting files) removes information from electronic storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing electronic storage media or IT equipment.

3.5. Overwriting Specifications. Overwriting is an approved method for sanitization of electronic storage media and IT equipment. Overwriting of data means replacing previously stored data on electronic storage media with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet the following specifications:

3.5.1. The data must be properly overwritten with a pattern. MHS requires overwriting with a pattern, and then its complement, and finally with a random pattern of 1's and 0's (e.g., overwrite first with "00110101," followed by "11001010," then "10010111").

3.5.2. Sanitization is not complete until all six passes of the three overwrite cycles are verified as completed.

3.5.3. The software must have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

3.5.4. The software must have the capability to overwrite using a minimum of three cycles (six passes) of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.

3.5.5. The software must have a method to verify that all data has been removed.

3.5.6. Media sectors not overwritten must be identified.

3.6. Degaussing Specifications. Degaussing is a process whereby the magnetic media is erased (e.g., returned to a zero state). Hard drives and other electronic storage media seldom can be used after degaussing. The degaussing (demagnetizing) method should only be used when the hard drive and other electronic storage media are inoperable and shall not be used for further service.

3.7. Extreme care should be used when operating degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. The use of a degausser **does not guarantee** that all data on the hard drive will be destroyed. Degaussing efforts should be audited periodically to detect equipment or procedure failures.

3.8. The following standards and procedures must be followed when hard drives and other electronic storage media are degaussed:

3.8.1. Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

3.8.2. Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

3.8.3. Hard disk platters must be in a horizontal direction during the degaussing process.

3.8.4. Degaussing products should be acquired from the National Security Agency's (NSA) Degausser Product List which can be obtained by contacting:

National Security Agency
Attn: S7 Media Technology Center
9800 Savage Road, Ft. George G. Meade, MD 20755-6877
(800)688-6115 (option 3) or (410)854-7661

3.9. Physical Destruction Specifications. Electronic storage media and IT equipment must be destroyed when it is defective, cannot be repaired, or cannot be sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive and other electronic storage media. This can be attained by removing the electronic storage media and hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

3.10. Sanitization of Other Computer Related Storage Media. If there is any risk of disclosure of DoD sensitive data on media other than computer hard drives, the appropriate sanitization methods as outlined in ASD (C3I) Memorandum, "Subject: Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001, and DoD 5220.22-M, "National Industry Security Program Operating Manual (NISPOM)," February 28, 2006, must be followed. Particular consideration and attention to detail should be acknowledged when sanitizing floppy disks, tapes, CDs, DVDs, optical disks, etc.

3.11. Memory components should also be sanitized before disposal or release. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

3.12. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing memory components for release. Memory components are categorized as either volatile or nonvolatile, as described below. Sanitization Procedures should be followed as specified in the table below.

3.12.1. Volatile memory components do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual

data (e.g., Static Random Access Memory (SRAM), Dynamic Random Access Memory (DRAM)).

3.12.2. 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.

| Media | Procedures |
|--------------------------------------|----------------------|
| Magnetic Tapes | |
| Type I* | a, b, or m |
| Type II** | a or b |
| Type III*** | m |
| Magnetic Disk | |
| Bernoulli's diskettes | m |
| Floppies | m |
| Non-Removable Rigid Disk | a, b, d, or m |
| Removable Rigid Disk | a, b, d, or m |
| Flash Drive | a, b, d, or m |
| Personal Digital Assistant (PDA) | a, b, d, or m |
| Optical Disk | |
| Read Many, Write Many | m |
| Read Only | m, n |
| Write Once, Read Many (WORM) | m, n |
| Memory | |
| Dynamic Random Access Memory (DRAM) | c, g, or m j or m |
| Electrically Alterable PROM (EAPROM) | h or m |
| Electrically Erasable PROM (EEPROM) | l, then c or m |
| Erasable Programmable ROM (EPROM) | c, then i or m |
| Flash EPROM (FEEPROM) | m |
| Programmable ROM (PROM) | a, b, c, or m |
| Magnetic Bubble Memory | a, b, e, or m |
| Magnetic Core Memory | c and f, or m |
| Magnetic Plated Wire | m |
| Magnetic Resistive Memory | c, g, or m |
| Nonvolatile RAM (NOVRAM) | m |
| Read Only Memory (ROM) | c, f, g, or m |
| Static Random Access Memory (SRAM) | |

Sanitization Procedures

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

*****Type III 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.**

| | |
|---|---|
| a | Degauss with a Type I degausser |
| b | Degauss with a 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 i. above, then c. above, three times |
| k | Perform an ultraviolet erase according to manufacturer's recommendation |
| l | Perform k above, 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 |

Sanitization Procedure Key

3.13. Certification of Sanitization. Sanitization may be required in instances other than disposal. The MHS requires the TMA Components to maintain documentation for all sanitization procedures. The sanitizing process must be documented on an additional form that explicitly outlines the method(s) used to expunge the data from the storage media, the type of equipment/media being sanitized, the name of the individual requesting sanitization, and the name of the person responsible for the sanitization. A form to capture the information shall be utilized to document this process (see Attachment 1).

3.14. The MHS Office of the Chief Information Officer/Information Assurance (OCIO/IA) requires that a copy of the proof of sanitization accompany all hard drives earmarked for disposal. This proof may be a copy of the entire “Record of IT Equipment Sanitization” or of Part II of the form. In instances where attaching the paper form to the equipment is not suitable, a label containing the required information may be affixed to the hard drive(s), equipment case (e.g., Central Processing Unit (CPU) box), or appropriate surface. The label must contain the name and signature of the person performing the sanitization, equipment identification and sanitization method used as provided in Part II of the “Record of IT Equipment Sanitization.” Equipment Serial and Inventory numbers must match those on the unit inventory.

3.15. For disposition outside the custody of the TMA Components and DoD, an adhesive label shall be affixed to the equipment case to record the sanitization process before transfer. For any remaining questions about leased equipment and equipment maintained through a service agreement, contact the Information Assurance Officer (IAO) or the Information Assurance Manager (IAM).

4. REFERENCES

1. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
2. DoD 5200.1-R, "Information Security Program," January 14, 1997
3. Public Law 100-235, "Computer Security Act of 1987," January 8, 1988
4. Privacy Act of 1974
5. ASD (C3I) Memorandum, "Subject: Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001
6. DoD 5220.22-M, "National Industry Security Program Operating Manual (NISPOM)," February 28, 2006
7. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

5. ACRONYMS

| | |
|----------|---|
| ASD(C3I) | Assistant Secretary of Defense, Command, Control, Communications and Intelligence |
| BIOS | Basic Input/Output System |
| CD | Compact Disk |
| CPU | Central Processing Unit |
| DAA | Designated Accrediting Authority |
| DoD | Department of Defense |
| DoDI | Department of Defense Instruction |
| DRAM | Dynamic Random Access Memory |
| DVD | Digital Versatile Disk |
| EAPROM | Electronically Alterable PROM |
| EEPROM | Electronically Erasable PROM |
| EPROM | Erasable Programmable Read Only Memory |
| FEPRM | Flash EPROM |
| HIPAA | Health Insurance Portability and Accountability Act |
| IA | Information Assurance |
| IAM | Information Assurance Manager |
| IAO | Information Assurance Officer |
| IS | Information System |
| IT | Information Technology |
| JMISO | Joint Medical Information Systems Office |
| MHS | Military Health System |

NISPOMNational Industry Security Program Operating Manual
NOVRAM.....Nonvolatile RAM
NSA.....National Security Agency
OCIO.....Office of the Chief Information Officer
PDA.....Personal Digital Assistant
PEO.....Program Executive Office
PHI.....Protected Health Information
PII.....Personally Identifiable Information
PROM.....Programmable Read Only Memory
ROM.....Read Only Memory
SRAM.....Static Random Access Memory
SI.....Sensitive Information
TMA.....TRICARE Management Activity
TRO.....TRICARE Regional Offices
WORM.....Write Once Read Many