



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. 9	
	EFFECTIVE DATE 07/19/05	REVISED DATE 10/10/08
<p>Subject:</p> <p style="text-align: center;">CONFIGURATION MANAGEMENT – SECURITY</p> <p style="text-align: center;">SOFTWARE USAGE AND MARKING</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 polices and procedures.

1.2. The term “MHS Information System (IS)” encompasses all automated IS applications, enclaves, outsourced information technology (IT)-based processes, and platform IT interconnections as defined in DoD Instruction (DoDI) 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003.

2. CONFIGURATION MANAGEMENT - SECURITY

2.1. PURPOSE

2.1.1. Configuration Management (CM) is a discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and to verify compliance with specified requirements. CM is paramount to maintaining a secure IA posture. The security elements in CM encompass the management of security features and assurance through the control of changes made to the software throughout the life cycle as part of the Defense-in-Depth strategy. Configuration control provides solid protective measures to ensure MHS ISs are protected against improper modifications prior to, during, and after system implementation. Strong security configuration management is a fundamental requirement for successful vulnerability management and must be tightly coordinated.

2.2. POLICY

2.2.1. A CM Plan shall be developed by the system owner to implement the appropriate level of change controls. The CM Plan shall include, but not be limited to:

2.2.1.1. An inventory of components.

2.2.1.2. Interconnectivity security requirements.

2.2.1.3. Peripherals inventory and configuration requirements.

2.2.1.4. Roles and responsibilities.

2.2.1.5. Automated tools.

2.2.1.6. Description of the baseline (e.g., software versions, patches, batch files, and environmental settings).

2.2.1.7. Internet Protocol (IP) address inventory.

2.2.1.8. Processes for keeping the security plan current.

2.2.1.9. Processes for disposal of electronic storage media and IT equipment in accordance with established DoD policy and MHS guidance.

2.2.1.10. Contingency operations to encompass security controls as outlined in the IA Controls located in DoDI 8500.2 for backup and recovery.

2.3. PROCEDURES

2.3.1. The Information Assurance Officer (IAO), System Owner/Program Manager (PM), and System Administrator (SA) shall ensure that a current and comprehensive baseline inventory of all hardware, software, and firmware (to include manufacturer, type, model, version, physical location, network topology or architecture, as well as installation manuals and procedures) required to support Department of Defense (DoD) IS operations and enclave operations is maintained by the Configuration Control Board (CCB), and as part of the Certification and Accreditation (C&A) documentation. A backup copy of the inventory shall be stored in a fire-rated container or in a secure location in another facility.

2.3.2. The IAO/SA shall maintain documentation of hardware and software configurations and diagrams essential to allow resumption of operations after a hardware/software failure.

2.3.3. The IAO/SA shall be involved in preparing a Continuity of Operations Plan (COOP)/Disaster Recovery/Contingency Plan to address Emergency Response, Backup Operations, and Recovery Actions. National Institute of Standards and Technology (NIST) Special Publication 800-34, “Contingency Planning Guide for Information Technology (IT) Systems,” provides instructions, recommendations, and considerations for government IT contingency planning. The IAO/SA shall ensure procedures are in place to assure the appropriate physical and technical protection of the backup and restoration hardware, software, and firmware, such as router tables, compilers, and other security-related system software. Continuity of Operations Plan (COOP)/Disaster Recovery/Contingency Plan shall be tested annually or when major changes occur.

2.3.4. No changes to the configuration of an IS or network shall be made until the IAO evaluates the effect(s) the proposed change shall have on the security countermeasures in place on the IS or network.

2.3.5. Any configuration changes that are made to an IS or network must be coordinated and approved by the CCB.

2.3.6. The IAO shall ensure configuration changes do not have an adverse impact on the security countermeasures of the IS or network.

2.3.7. During the life cycle of the IS or network, a CM system shall be in place for security-relevant hardware, software, and firmware. Detailed instruction regarding the sanitization of electronic storage media and disposition of IT equipment shall be clear.

2.3.8. The PMs, IAOs, and SAs shall maintain control of changes to the formal security configuration model, the descriptive and formal top-level specifications, other design information, implementation documentation, source code, the running version of the object code, and documentation.

2.3.9. Tools shall be available and maintained under strict configuration control for comparing an updated version of software with the previous version. These tools must ascertain that only the intended changes have been made in the code that shall be used as the new version of the IS or network.

2.3.10. The IAO shall maintain an accurate inventory of disposed and sanitized electronic media. Inventory should include, at a minimum:

2.3.10.1. Date of disposition or sanitization.

2.3.10.2. Location of disposition or sanitization.

2.3.10.3. Type of electronic storage media (e.g., magnetic diskettes, hardware, compact discs (CDs)).

2.3.10.4. Current status.

2.3.11. The IAO shall document the implementation of all changes in the C&A documentation.

3. SOFTWARE USAGE

3.1. PURPOSE

3.1.1. This implementation guide provides specific policy on software use for DoD systems, to include policies governing software purchased or developed by the government in accordance with DoDI 8500.2. The acquisition of all IA and IA-enabled Commercial-off-the-Shelf (COTS) IT products is limited to products that have been evaluated or validated through one of the following sources – the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the National Information Assurance Partnership (NIAP) Evaluation and Validation Program, or the Federal Information Processing Standards Publications (FIPS) validation program.

3.2. POLICY

3.2.1. DoDD 8500.01E, “Information Assurance,” dated October 24, 2002, certified current as of April 23, 2007, requires that all IA or IA-enabled products incorporated into DoD information systems must comply with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, “Revised Fact Sheet National Information Assurance Acquisition Policy,” July 2003. Products must be satisfactorily evaluated and validated either:

3.2.1.1. Prior to purchase.

3.2.1.2. As a condition of purchase, the vendor’s products will be satisfactorily evaluated and validated.

3.2.2. Purchase contracts shall specify that product validation will be maintained for subsequent releases.

3.2.3. Copyright and licensing agreements must be honored and the software must be tracked to ensure compliance. Managers who purchase software protected by quantity licenses must ensure that a system is in place to control copying and distribution.

3.3. PROCEDURES

3.3.1. IAOs shall establish procedures to ensure that only software licensed to the government is installed on MHS ISs.

3.3.2. All versions and copies of software shall be controlled and documented through CM accounts.

3.3.3. Instructions for restart and recovery procedures, restrictions on source code access, and system utility access shall be maintained.

3.3.4. Copyrighted software products must not be reproduced except to the limit provided by contract (e.g., archive copy for backup).

3.3.5. All personnel shall abide by copyright protection laws or contractual requirements when using copyrighted software. The IAO shall ensure users (including contractors) are educated in these requirements during initial and refresher security training.

3.3.6. Operating System (OS) software shall have the capability to identify, journal, report, and assign accountability for the OS functions performed or attempted by a user (including contractors). The OS software shall have the capability to deny specific rights and privileges to unauthorized users (including contractors). As a minimum, the SA shall comply with this implementation guide and DoDI 8510.01, "Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007. Depending on the OS, more stringent internal policies may apply. The SA shall adhere to the minimum requirements below:

3.3.6.1. Display a warning banner at logon to indicate that access is restricted to authorized users for legitimate work purposes only and subject to monitoring by system administrators.

3.3.6.2. Prevent authorized users (including contractors) from accessing and executing privileged user programs and instructions.

3.3.6.3. Ensure the OS software has the capability of backing up information in a secure environment.

3.3.7. Application software may be installed by the SA after complying with MHS policy as listed below:

3.3.7.1. Define security requirements and specifications, functional requirements, and obtain approval from the appropriate approving authority.

3.3.7.2. Conduct periodic design reviews during the developmental phases to assure the proposed design complies with functional and security requirements as specified.

3.3.7.3. Thoroughly test new or substantially modified sensitive applications prior to implementation to verify that the user functions and the required administrative, technical, and physical safeguards are present and operationally adequate.

4. MARKING

4.1. PURPOSE

4.1.1. This implementation guide provides policy for the proper marking and labeling of protected health information (PHI), sensitive information (SI), and hardware, as required. These measures are necessary to help prevent the loss, misuse, unauthorized access to, or modification of PHI/SI.

4.2. POLICY

4.2.1. As required by DoD 5200.1-R, "Information Security Program," 14 January 1997, sensitive unclassified information is to be marked to accurately reflect the sensitivity of the information. The marking may be automated (e.g., the IS has a feature that produces the markings) or may be done manually. When SI is included in DoD documents, it shall be marked as if the information were For Official Use Only (FOUO) (see DoD 5400.7-R, "DoD Freedom of Information Act Program," September 1998, for further FOUO guidance). When PHI/SI is included in DoD documents, it shall be handled in accordance with DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003.

4.2.2. MHS ISs that store, process, transmit, or display data in any form or format that is not approved for public release, or is PHI/SI, shall comply with all requirements for marking and labeling contained in this implementation guide and other policy and guidance documents, such as DoD 5200.1-R and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Information Assurance Manager (IAM), IAO, and SA shall implement procedures for all users (including contractors) to ensure markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions as specified in DoDI 8500.2, "Information Assurance (IA) Implementation," 6 February 2003. Disposition of hard copy output containing PHI/SI shall be in accordance with DoDI 8500.2 and DoD 6025.18-R.

4.3. PROCEDURES

4.3.1. Mark hardware components of an IS with a conspicuous external label indicating the highest classification/sensitivity of information that can be processed on the IS. The notice may consist of either permanent markings or a label. Components include input/output devices that retain PII/PHI/SI, workstations, terminals, personal computers, stand-alone personal computers, and word processors used as terminals.

4.3.2. Mark, physically control, and safeguard removable media in a manner prescribed for the highest classification/sensitivity recorded on them until the media is

destroyed or sanitized. Users (including contractors) shall also control and safeguard removable media in the same manner as described above.

4.3.3. Mark non-removable media with external labels indicating if PHI/SI is processed and its associated security markings, such as handling caveats and dissemination control labels. If it is not cost-effective or practical to mark the non-removable media itself, the labels described in the following paragraphs must be placed in a visible location on the cabinet housing the media.

4.4. Unclassified IT equipment and electronic storage media may be selected for reuse, repair, replacement, or removal from service for a variety of reasons. MHS shall comply with the Assistant Secretary of Defense (ASD) Memorandum, "Disposition of Unclassified DoD Hard Drives," June 4, 2001, and DoDI 8500.2, Enclosure 4, Attachments 3 and 5, as applicable. The MHS IAO shall ensure the following procedures are enforced:

4.4.1. Government-Owned IT Equipment and Electronic Storage Media – Operational IT equipment and electronic storage media that will be reused must be overwritten in accordance with DoD policy prior to transfer. If the IT equipment and electronic storage media become inoperable, have reached the end of their useful life, or are removed from service completely, they should be destroyed or degaussed in accordance with DoD policy.

4.4.2. Leased Computers – If the leased IT equipment and electronic storage media are operational and are being relocated within a contract umbrella (e.g., it will remain under the authority of the DoD leasing agent or seat manager), overwriting is not required, unless it has been used to process PHI/SI. If the IT equipment and electronic storage media have processed PHI/SI, the leasing agent shall overwrite, certify, and label them in accordance with DoD policy. If the IT equipment and electronic storage media are to be redirected from the contract umbrella, the leasing agent shall overwrite, certify, and label them in accordance with DoD policy. If the leased IT equipment and electronic storage media are inoperable, the contractor shall make a determination as to whether they are repairable or whether they should be removed from service.

4.4.3. Contractor-Owned Computers – Contractor-owned operational IT equipment and electronic storage media containing DoD/MHS data which are selected for reuse must be overwritten in accordance with DoD policy prior to transfer. If the IT equipment or other electronic storage media is removed from service completely, it should be destroyed or degaussed in accordance with DoD policy. Inoperable IT equipment and other forms of electronic storage media that have reached the end of their useful life shall be destroyed or degaussed in accordance with DoD policy before disposal.

4.4.4. Warranty Actions – The warrantor shall make a determination as to whether the IT equipment and electronic storage media should be repaired and returned to the original government user, repaired but redirected to another user, or permanently removed from service. The process and procedure for handling inoperable IT equipment

and electronic storage media returned for warranty action are the same as those for inoperable IT equipment and electronic storage media that is returned to the contractor under lease agreements and are handled in accordance with DoD policy.

4.4.5. Physical destruction of any IT equipment and other forms of electronic storage media shall be carried out in accordance with DoD policy.

4.5. Handling of SI and PHI

4.5.1. All patient information processed and output (printed) by TMA Components and contractor ISs is sensitive and shall be protected, marked, or labeled in accordance with DoD policy for the protection of FOUO information, which is a subset of SI, and in accordance with HIPAA for the protection of PHI/SI.

4.5.2. TRICARE beneficiaries have a right to privacy of their information. Accordingly, controls must be established to affect this policy.

4.5.3. A Privacy Act Statement shall be provided to the individual in accordance with the requirements of the Privacy Act when information is obtained from an individual. If the organization discloses patient PHI/SI, then that disclosure must be recorded.

4.5.4. Privacy Act data must be labeled, “For Official Use Only. Warning: This information requires protection under the Privacy Act.”

4.5.5. IS users (including contractors) shall ensure devices that display or output PHI/SI in human-readable form are positioned to deter or prevent unauthorized individuals from reading the information.

4.5.6. FOUO material and PHI/SI are information that have not been assigned a security classification, but which may be withheld from the public for one or more reasons cited in the Freedom of Information Act exemptions list or the HIPAA. The IAO shall use DoD 5400.7-R, DoD 6025.18-R, and the instructions below to handle and control PHI/SI.

4.5.7. FOUO information status should be indicated by markings when present in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information. The marking may be automated or done manually, such as with a stamp.

4.5.8. Unclassified documents and material containing FOUO information should be marked as follows:

4.5.8.1. Mark documents “FOR OFFICIAL USE ONLY” at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).

4.5.8.2. Mark pages of the document that contain FOUO information “FOR OFFICIAL USE ONLY” at the bottom.

4.5.8.3. Mark material other than paper documents (e.g., slides, computer media, films) containing FOUO information to alert the holder or viewer to that fact.

4.5.8.4. Put an expanded marking on the face of FOUO documents and material transmitted outside the DoD so that non-DoD holders understand the status of the information. Use a statement similar to this one: “This document contains information exempt from mandatory disclosure under the Freedom of Information Act. Exemption(s) ____ (Insert Exemption/Exemption Number here) apply.”

4.5.8.5. The IAO shall implement procedures to ensure FOUO information or PHI/SI shall not be posted to publicly accessible Web sites.

4.5.9. Documents or material containing PHI/SI shall be destroyed by shredding or placed in an official DoD burn bag, as directed by DoD policies and procedures.

4.5.10. Storage of Information and Material

4.5.10.1. Develop and implement procedures to ensure the proper handling and storage of information takes place, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.

4.5.10.2. Store equipment in approved containers or facilities with maintenance and accountability procedures as directed by DoD 5200.1-R.

4.5.10.3. Adhere to the DoD Storage of Information and Material requirements.

5. **REFERENCES**

1. Assistant Secretary of Defense (ASD) Memorandum, “Disposition of Unclassified DoD Hard Drives,” 4 June 2001
2. DoD 5200.1-R, “Information Security Program,” 14 January 1997
3. DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 1998
4. DoD 6025.18-R, “DoD Health Information Privacy Regulation,” January 2003
5. DoDD 8500.01E, “Information Assurance (IA),” 24 October 2002, certified current as of April 23, 2007
6. DoDI 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003

7. DoD 8510.01, “Department of Defense Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007
8. NSTISSP No. 11, “Revised Fact Sheet National Information Assurance Acquisition Policy,” July 2003
9. Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,” 21 August 1996
10. NIST Special Publication 800-34, “Contingency Planning Guide for Information Technology (IT) Systems,” June 2002

6. ACRONYMS

ASD.....	Assistant Secretary of Defense
C&A.....	Certification and Accreditation
CC	Common Criteria
CD.....	Compact Disc
CCB.....	Configuration Control Board
CM	Configuration Management
COOP	Continuity of Operations Plan
COTS	Commercial-off-the-Shelf
DIACAP.....	Department of Defense Information Assurance Certification and Accreditation Process
DoD.....	Department of Defense
DoDD.....	Department of Defense Directive
DoDI	Department of Defense Instruction
FIPS.....	Federal Information Processing Standards
FOUO.....	For Official Use Only
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IAM.....	Information Assurance Manager
IAO	Information Assurance Officer
IP	Internet Protocol
IS	Information System
IT.....	Information Technology
JMIS	Joint Medical Information Systems Office
MHS.....	Military Health System
NIAP	National Information Assurance Partnership
NIST.....	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OS	Operating System
PEO.....	Program Executive Office
PHI	Protected Health Information
PII.....	Personally Identifiable Information
PM.....	Program Manager

SASystem Administrator
SI.....Sensitive Information
TMA.....TRICARE Management Activity
TRO.....TRICARE Regional Offices