



TRICARE
MANAGEMENT
ACTIVITY

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS**

SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

JUN 19 2009

**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 Information Assurance Policy Guidance and Military
Health System Information Assurance Implementation Guides**

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

Implementation Guide No. 3, "Incident Reporting"
Implementation Guide No. 4, "Network Security Accountability – Employee Behavior"
Implementation Guide No. 8, "Certification & Accreditation"
Implementation Guide No. 14, "INFOCON"

The MHS IA Policy Guidance and 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 Policy Guidance and IA Implementation Guides are policy for all TRICARE Management Activity (TMA) Directorates, TRICARE Regional Offices (TRO), 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 polices and procedures.

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


for 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. 4	
	EFFECTIVE DATE 07/19/05	REVISED DATE 03/25/09
<p>Subject:</p> <p style="text-align: center;">NETWORK SECURITY ACCOUNTABILITY EMPLOYEE BEHAVIOR</p>		

1. PURPOSE AND SCOPE

1.1. The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (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 (CIO) of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

1.2. This implementation guide provides the rules and policies governing the behavior of the employees of the TMA Components who manage, design, develop, operate, and access Department of Defense (DoD) Information Systems (ISs), or access DoD data, while accessing or using DoD information technology resources.

2. POLICY

2.1. The DoD 5500.7-R, “Joint Ethics Regulation (JER),” August 1993 (Changes 1-6), Section 2-301, directs that the use of federal government resources, including personnel, equipment, and property (e.g., computers, e-mail, and Internet systems), “shall be for official use and authorized purposes only.” “Official use” refers to uses that directly further the interests of the DoD and the duties prescribed for the individual position. “Authorized purposes” refers to personal use within specified limits as permitted by an appropriate level supervisor. The specified limits are described below:

2.1.1. Does not adversely affect performance of official duties.

2.1.2. Is of reasonable duration and frequency.

2.1.3. Whenever possible, is made during the member’s personal time (before/after duty hours, during lunch, or authorized breaks).

2.1.4. Serves a legitimate DoD interest.

2.1.5. Does not reflect adversely on the DoD or MHS.

2.1.6. Does not overburden the communications system.

2.1.7. Results in no significant additional cost to the DoD or MHS.

2.2. Authorized Purposes. The MHS IA Implementation Guide for Network Security Accountability/Employee Behavior establishes boundaries for limited personal use of DoD resources consistent with the above-listed limitations. Limited personal use would include the following activities (e-mail or Web based):

2.2.1. E-mailing short messages to a relative or colleague.

2.2.2. Receiving e-mail (as long as comparable receipt would be acceptable via telephone, and is no more disruptive than a telephone call).

2.2.3. Announcing MHS-related activities (e.g., office luncheons, retirement or departure events, and holiday office parties).

2.2.4. Making a medical, dental, auto repair, or similar appointment.

2.2.5. Accessing the Internet for professional development purpose.

2.2.6. Checking investment status (e.g., stock prices) or authorizing a financial transaction.

2.2.7. Reading a news or business magazine.

2.3. Workstation Position. In order to protect sensitive information (SI) during the performance of official duties, users must position monitors to prevent unintentional viewing.

2.4. Authentication. System users will access TMA ISs via Common Access Cards (CACs) at all times. Attempts to circumvent authentication measures constitute a violation of TMA and DoD policy.

2.5. Software License. System users, who illegally acquire and/or use unauthorized, unlicensed copies of software, shall be held accountable under U.S. copyright law. Violations might result in civil/criminal penalties and employee termination.

2.6. Modification. System users are restricted from adding or removing devices or hardware from TMA ISs.

2.7. Off-site computing. Remote access is reserved for performance of official duty only (e.g., mission-related dial-in from home or temporary duty (TDY) location). Personal use of the

network remote access capability is prohibited. Only government equipment (e.g. assigned laptops) may be used to access TMA networks.

2.8. Removal of Sensitive Data. No sensitive data (including Protected Health Information (PHI) or Personally Identifiable Information (PII)) may be removed without Designated Accrediting Authority (DAA) approval. DoD defines PII as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

2.9. PII - MHS ISs containing DoD data identified as PII shall be categorized in one of the following categories:

2.9.1. High Impact – A compilation of 500 or more electronic records containing PII stored on a single device, accessible through an application or service, or less than 500 electronic records when the information owner requires additional protection measures.

2.9.2. Moderate Impact – Any PII electronic records containing PII not identified as High impact.

2.10. High Impact PII records shall not be routinely processed or stored on mobile computing devices or removable media without express approval of the DAA.

2.11. MHS ISs containing DoD data identified as PII, not explicitly cleared for public release, shall be protected in accordance with appropriate confidentiality and sensitivity level.

2.12. Any mobile computing device containing High Impact PII removed from the protected workplace, including those approved for routine processing, shall:

2.12.1. Be signed in and out with a supervising official designated in writing.

2.12.2. Require DoD-approved PKI certification to be accessed.

2.12.3. Enable screen-lock functionality with a specified period of workstation inactivity within fifteen minutes.

2.13. Encryption of sensitive data. Encryption of data for transmission and storage to and from mobile/wireless devices is required. Authorized Users of mobile/wireless are required to ensure all sensitive information (e.g., Personally Identifiable Information (PII), Protected Health Information (PHI)) is encrypted, whether data is in transit or stored at rest. Encryption is required regardless of storage media type. Types include, but are not limited to; Portable Electronic Devices (PEDs), Personal Digital Assistants (PDAs), cell phones, zip and compact disks, magnetic floppy disks, removable disk drives, and laptop computers.

2.13.1. The use of removable flash memory (thumb drives, memory sticks, and flash memory) is prohibited on all DoD Networks.

2.14. Unauthorized/Inappropriate Activity. The following list provides examples (not all-inclusive) of uses that would be unauthorized and inconsistent with the appropriate use of TMA resources:

2.14.1. Soliciting business, advertising, or engaging in other selling activities in support of private business enterprises or outside employment.

2.14.2. Fundraising activities not sanctioned by TMA.

2.14.3. Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity, including campaign fundraising.

2.14.4. Use of a DoD network as a staging ground or platform to gain unauthorized access to other systems.

2.14.5. Attempting to circumvent, disable, or compromise TMA Component security and authentication measures.

2.14.6. Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, and/or any other prohibited or illegal activities.

2.14.7. Accessing, creating, downloading, viewing, storing, copying, or transmitting sexually oriented or racist materials.

2.14.8. Participating in “spamming”; that is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail.

2.14.9. Participating in “letter-bombing”; that is, sending the same e-mail repeatedly to one or more recipients to interfere with the recipient’s use of e-mail.

2.14.10. Downloading shareware/freeware software or executable programs (e.g., .EXE, .COM, .BAT, or script.INI files).

2.14.11. Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to terrorist activities.

2.14.12. Creating, copying, or transmitting chain letters or other unauthorized mailings regardless of the subject matter.

2.14.13. Accessing or participating in Internet Relay Chat sessions.

2.14.14. Posting MHS information to external newsgroups, bulletin boards, or other public forums without authority.

2.14.15. Sending, whether initiating or replying to, inappropriate messages or messages containing inappropriate language.

2.14.16. Accessing sites known for hacker attacks or hacker activity.

2.14.17. Opening e-mail attachments from unknown or questionable sources. End users should be aware of phishing attempts in e-mails or fraudulent websites that are attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

2.14.18. Transmitting sensitive information (including PHI) via the Internet without ensuring appropriate security controls (e.g., encryption) are in place.

2.15. Consent to Monitoring. Use of DoD resources and equipment is neither private nor anonymous. In accordance with federal laws and regulations, use of such resources may be monitored.

2.15.1. Personnel should remember that electronic transmissions can create a permanent record of the information transmitted. Even an activity intended to be a temporary transfer of information may be maintained as permanent record.

2.16. Sanctions for Misuse. Military, civilian personnel, and contractors will be subject to administrative and/or judicial sanctions if they knowingly, willfully or negligently compromise, damage or place at risk DoD information systems or data. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access. Action may also be taken under the Uniform Code of Military Justice (UCMJ) and applicable federal or state law.

2.17. Administrative and/or judicial sanctions will be enforced by the Chain of Command.

3. PROCEDURES

3.1. The MHS CIO shall enforce compliance with restrictions on the use of DoD resources. Compliance shall be enforced through a variety of means including:

3.1.1. Administrative sanctions specifically related to the system (e.g., loss of system privileges).

3.1.2. General sanctions as are imposed for violating other rules of conduct regarding system use.

3.1.3. Civil and criminal penalties.

3.2. TMA shall assign government laptops to users that require remote access to TMA systems. These laptops must be accessible only by CAC.

3.3. Supervisors must ensure individuals in the office environment are made aware of directorate or office-specific policies. Supervisors must report any unauthorized activities or suspected misuse to the Information Assurance Manager (IAM).

3.3.1. Supervisors must submit written approval to the DAA before allowing a user(s) to remove sensitive data (including PHI) from TMA facilities. The submitted approval must specify date, type of data, reason for being removed from the facility, and identifying data from the user's assigned laptop.

3.4. As a requirement for network access, users shall be required to sign the Network Security Agreement and System User Agreement that outlines:

3.4.1. User responsibilities.

3.4.2. Potential sanctions for non-compliance with established rules.

3.5. Users must sign a current Network Security Agreement acknowledging that they are responsible for maintaining the physical security and confidentiality of sensitive information.

3.6. Users must complete annual security training in order to maintain access to the network.

3.7. Users are required to comply with the parameters of this policy and to report misuse to their supervisors. Users are reminded to apply the same standards governing use of the TMA Network to the use of any DoD resource regardless of location (i.e., TDY or other government sites). Questions regarding "authorized purposes" or "use limits" should be directed to the supervisor who shall forward them to the IAM for action.

4. REFERENCES

1. DoD CIO Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
2. CJCSM 6510.01 CH 3, "Defense-In-Depth: Information Assurance (IA) and Computer Network Defense," Current as of March 14, 2007
3. DoDD 5400.11, "DoD Privacy Program," May 8, 2007
4. DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1993 (Changes 1-6)
5. DoDD 5500.7, "Standards of Conduct," November 29, 2007
6. DoDD 8500.01E, "Information Assurance (IA)," October 24, 2002, certified current as of April 23, 2007
7. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
8. DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003

5. ACRONYMS

CACCommon Access Card

CIO.....	Chief Information Officer
DAA.....	Designated Accrediting Authority
DoD.....	Department of Defense
DoDD.....	Department of Defense Directive
E-mail.....	Electronic Mail
IA.....	Information Assurance
IAM.....	Information Assurance Manager
IS.....	Information System
JER.....	Joint Ethics Regulation
JMIS.....	Joint Medical Information Systems
MHS.....	Military Health System
PDA.....	Personal Digital Assistant
PED.....	Portable Electronic Device
PEO.....	Program Executive Officer
PHI.....	Protected Health Information
PII.....	Personally Identifiable Information
PKI.....	Public Key Infrastructure
SI.....	Sensitive Information
TDY.....	Temporary Duty
TMA.....	TRICARE Management Activity
TRO.....	TRICARE Regional Offices
UCMJ.....	Uniform Code of Military Justice