

 <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS)</p> <p style="text-align: center;">INFORMATION ASSURANCE (IA)</p> <p style="text-align: center;">IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 7	
	EFFECTIVE DATE 07/19/05	REVISED DATE 02/22/12
<p>Subject:</p> <p style="text-align: center;">DATA INTEGRITY</p>		

1 PURPOSE AND SCOPE

1.1 The provisions of this guide are policy for all TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO); and the Military Electronic Health Record Center (MEHRC) (hereafter collectively 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 This implementation guide outlines safeguards for detecting and minimizing the potential unauthorized modifications or any other form of malicious actions or corruption to data contained in MHS information systems (IS). This also includes threats, corruption, or destruction of data that is accidental in nature. Data integrity is defined as system data remaining unchanged from its original source through accidental or malicious modifications, alterations, or destruction. Data integrity has two main objectives:

1.2.1. Ensuring that the data has not been altered in an unauthorized manner while in transit, during storage, or while being processed.

1.2.2. Ensuring a system, while performing its intended processes and applications, provides support to authorized users free from unauthorized manipulation.

1.3 Exploitation of vulnerabilities associated with data or system integrity may result in a disruption or denial of service, and/or unauthorized modification of user or network information and network services. It is the responsibility of the MHS IA Program Office to ensure protective measures are in place, coupled with industry best practices, to maintain the appropriate level of data and system integrity to include while data is at rest.

2 GUIDANCE

2.1 The MHS requires implementing data and system integrity measures to protect DoD data from unauthorized manipulation, intentional or unintentional alteration, or destruction. The MHS shall utilize access control mechanisms, virus protection programs, and

information monitoring capability as required by DoDI 8500.2, “Information Assurance (IA) Implementation,” IA controls.

2.2 MHS ISs containing DoD data identified as Personally Identifiable Information (PII) (any information about and individual that includes, but is not limited to; education, financial transactions, or medical, criminal, or employment history, which can be used to distinguish or trace an individual’s identity, such as their name, social security number, date and place of birth, etc.), not explicitly cleared for public release, shall be protected in accordance with appropriate confidentiality and sensitivity level at all times, to include while data is at rest (e.g., during transport to a storage facility or while in storage).

2.3 MHS ISs containing DoD data identified as PII shall be categorized on one of the two categories:

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

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

2.4 It is MHS Policy that:

2.4.1 The Information Assurance Manager (IAM) shall ensure that access to all DoD and MHS information is determined by its classification, sensitivity, and need-to-know. Need-to-know is established by the information owner and is enforced by discretionary or role-based access controls.

2.4.2 The IAO shall ensure policies and procedures are implemented for ISs that handle DoD data to allow access only to those persons or software programs that have been granted access rights.

2.4.3 The IAO shall establish and enforce access controls for all shared or networked file systems and internal Web sites, whether classified, sensitive, or unclassified.

2.4.4 The IAO shall ensure information owners assign impact categories for PII records.

2.4.5 The IAO shall ensure supervisors establish logging and tracking procedures for PII removed from a protected work place. This includes the transport of data at rest to or from a storage facility.

2.4.6 All internal classified, sensitive, and unclassified Web sites shall be organized to provide at least three distinct levels of access:

2.4.6.1 Open Access – General information made available to all DoD and TMA Component authorized users with network access. This access does not require an audit transaction.

- 2.4.6.2 Controlled Access – Information made available to all DoD and TMA Component authorized users upon the presentation of an individual authenticator. This access shall be recorded in an audit transaction.
- 2.4.6.3 Restricted Access – Need-to-know information made available only to an authorized community of interest. Authorized users must present an individual authenticator and have a demonstrated or validated need-to-know. All access to need-to-know information and all access attempts shall be recorded in audit transactions.
- 2.4.7 The IAO shall establish appropriate control mechanisms to ensure that data in transit or at rest is properly disposed of by authorized personnel only.
- 2.4.8 The IAO shall establish and enforce procedures to verify the identity of a person or entity seeking access to data.
- 2.4.9 The IAO shall maintain and enforce procedures to establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process, or data.
- 2.4.10 The IAO shall ensure that a controlled interface is implemented for interconnections among DoD ISs operating at different classifications levels or between DoD and non-DoD systems or networks.
- 2.4.11 The IAO shall determine the need for and the strength of the mechanism for automatic logoff based on DoD direction and the organization’s risk assessment, and shall document policies and procedures for terminating an electronic session after a predetermined time of inactivity.
- 2.4.12 The IAO shall determine the appropriate mechanism for encrypting and decrypting sensitive electronic data including personally identifiable information (PII) and protected health information (PHI) in transit, at rest, in transport, or storage in accordance with DoDI 8500.2 and Federal Information Processing Standards (FIPS) 140-2, “Security Requirements for Cryptographic Models,” December 3, 2002.
- 2.4.13 The IAO shall implement system resource control and object access to ensure all authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system’s pool of unused objects. No information, including encrypted representations of information, produced by a prior subject’s actions is available to any subject that obtains access to an object released back to the system. There must be no residual data from the former object.
- 2.4.14 The IAO shall implement electronic mechanisms to confirm data has not been altered or destroyed in an unauthorized manner.
- 2.4.15 Virus protection shall be installed, enabled, maintained, and have the ability to be automatically updated on all MHS ISs.
- 2.4.16 TMA Components shall review system records on a weekly basis, or more frequently if deemed necessary.

2.4.17 TMA Components shall implement and maintain an information security monitoring capability to ensure all systems they operate and/or control are regularly monitored and protected by intrusion detection systems.

2.4.18 Successive logon attempts shall be controlled using one or more of the following:

2.4.18.1 Access is denied after three unsuccessful logon attempts in accordance with Chairman, Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND)," March 25, 2003.

2.4.18.2 A time-delay control system is employed.

2.4.18.3 The system provides a capability to control the number of logon sessions if the system allows for multiple-logon sessions for each User Identification (User ID).

3 PROCEDURES

3.1 The IAO shall manage authorized user accounts for MHS systems, including configuring access controls to enable access to authorized information and removing authorization when access is no longer needed. The responsibility may be delegated to the System Administrator (SA).

3.2 Limit users to three attempts when logging onto an MHS IS. After the maximum number of incorrect attempts, the system shall lock out the user until an administrator unlocks the account. Action from the IAO shall be required to reactivate the account. This action prevents outsiders from accessing the IS by using a known User ID and trying to guess the password.

3.3 Enable screen-lock functionality on all MHS workstations and any workstation that accesses DoD information. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, hiding what was previously visible. Such a capability is enabled by either explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator.

3.4 The screen lock function shall not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

3.5 In addition to the DoD 5500.7-R, "Joint Ethics Regulation (JER)," requirements, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule provides specific security standards for the protection of workstations that process PHI. These include:

3.5.1 Locking the workstation before leaving the workstation unattended.

3.5.2 Positioning the workstation to obstruct unauthorized viewing and access.

3.6 The IAO shall establish Web site administration policy and procedures consistent with the "DoD Web Site Administration Policies and Procedures," 25 November 1998, as amended on 11 January 2002.

- 3.7 The IAO shall establish system Access Control Lists (ACLs) to restrict traffic to only that which is required to pass through the Web site.
- 3.8 All MHS IS users shall take precautions to prevent viruses from infecting MHS ISs. The IAO shall ensure all developers are protecting source or executable code by utilizing 'checksum' or another safeguard to ascertain approved code is not altered.
- 3.9 The IAO shall ensure all software must be approved and scanned for viruses before loaded on a TMA system.
- 3.10 All MHS IS users are to report suspected suspicious activity to the local supervisor or IAO. Suspicious activity includes, but is not limited to:
 - 3.10.1 Suspected misuse or unauthorized use of government resources.
 - 3.10.2 Use of an IS account and password by another party.
 - 3.10.3 Illegal copying of software.
 - 3.10.4 Abnormal activity on an IS, which may indicate the presence of a computer virus or malicious code.
- 3.11 Only approved, virus scanned software shall be installed on workstations.
- 3.12 No software that changes the security posture shall be installed on MHS ISs without approval from the appropriate Designated Accrediting Authority (DAA).
- 3.13 The IAO shall ensure backup copies of protected system files, critical data files, and applications (backup copies of applications for archival purposes generally do not represent a copyright violation) are created and stored on electronic storage media in a secure location and are not collocated with the originals. A network/SA should have a backup copy of every software program each time it is modified in accordance with established software development procedures and controls. This provides some assurance that a clean backup exists in the event a virus or malicious code is detected. The SAs should also scan the servers for viruses or malicious code monthly.
- 3.14 The IAO shall ensure encryption and decryption standards are in compliance with the FIPS 140-2 and DoDI 8500.2. The IAO shall require and ensure encryption policies and procedures are documented.
- 3.15 Users shall not use electronic storage media from home systems or other external sources that have not been approved and scanned for viruses. Users shall not duplicate copyrighted software or share software with other employees.
- 3.16 High Impact PII records shall not be routinely processed or stored on mobile computing devices or removable media without express approval of the DAA.
- 3.17 Any mobile computing device containing High Impact PII removed from the protected workplace, including those approved for routine processing, shall:
 - 3.17.1 Be signed in and out with a supervising official designated in writing.
 - 3.17.2 Require DoD-approved PKI certification to be accessed.
 - 3.17.3 Enable screen-lock functionality with a specified period of workstation inactivity within fifteen minutes.

- 3.18 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., Privacy, PHI) is encrypted, whether data is in transit or stored at rest, regardless of storage media type. Types include, but are not limited to; Portable Electronic Devices (PEDs), Personal Digital Assistants (PDAs), cell phones, flash drives, memory sticks, zip and compact disks, magnetic floppy disks, and removable disk drives, and laptop computers.
- 3.19 In case of an incident or catastrophic failure, routine data backup and detailed disaster recovery plans shall be available to retrieve exact copies of lost data and ensure data integrity.
- 3.20 Users shall be trained annually in accordance with DoD 8570.1. At the minimum, data integrity training shall include appropriate security practices for operating an MHS workstation and IS, guarding against, detecting, and reporting suspicious IS activities.

4 REFERENCES

- 1) DoD 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- 2) DoD Chief Information Officer (CIO) Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
- 3) DoDD 8500.01E, "Information Assurance (IA)," October 24, 2002
- 4) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- 5) DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007
- 6) DoDD 5500.7, "Standards of Conduct," August 30, 1993
- 7) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1993 (Changes 1-6)
- 8) FIPS 140-2, "Security Requirements for Cryptographic Models," May 25, 2001
- 9) "DoD Web Site Administration Policies and Procedures," November 25, 1998, as amended on January 11, 2002
- 10) Health Insurance Portability and Accountability Act of 1996: Title 45 Code of Federal Regulations Part 164, "Security and Privacy," February 23, 2003
- 11) CNSSI No. 4009, "National Information Assurance (IA) Glossary," April 2010

5 ACRONYMS

CIO.....	Chief Information Officer
CJCSM.....	Chairman, Joint Chiefs of Staff Manual
CND	Computer Network Defense
DoD.....	Department of Defense
DoDD.....	Department of Defense Directive
DoDI	Department of Defense Instruction
FIPS.....	Federal Information Processing Standard
IA	Information Assurance
IAM.....	Information Assurance Manager
IS	Information System
JER.....	Joint Ethics Regulation
JMISO.....	Joint Medical Information Systems Office
MHS	Military Health System
PDA.....	Personal Digital Assistants
PED.....	Portable Electronic Devices
PEO.....	Program Executive Office
PHI.....	Protected Health Information
PII.....	Personally Identifiable Information
SA	System Administrator
TMA.....	TRICARE Management Activity
TRO.....	TRICARE Regional Offices
User ID.....	User Identification