

 <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. 6	
	EFFECTIVE DATE 07/19/05	REVISED DATE xx/xx/xx
<p>Subject:</p> <p style="text-align: center;">WIRELESS LOCAL AREA NETWORKS (WLANs)</p>		

1 PURPOSE AND SCOPE

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.

1.1 The purpose of this implementation guide is to:

- a. Support references (a) through (m) concerning wireless transmission of all MHS data over a wireless 802.11X LAN. The protection of all wirelessly transmitted data and packet information, to include source and destination Internet Protocol (IP) addresses, mitigates the risk of compromising Sensitive Information (SI), Personal Identifiable Information (PII) or Protected Health Information (PHI) over a wireless network connection.
- b. Assign responsibilities to ensure that sufficient defense-in-depth security safeguards are implemented to prevent the compromise of one system's security assurance by vulnerabilities of interconnected systems introduced via wireless communications.
- c. Promote interoperability using open standards for commercial wireless implementations throughout the MHS.
- d. Promote the use of a Knowledge Management (KM) process for the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the MHS.

1.2 This guide recommends an approach that incorporates existing Defense Information Systems Agency (DISA), Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and Service policy and guidance with MHS-specific guidance to provide a foundation for a comprehensive risk mitigation strategy that ensures sensitive data, including PHI, transmitted via wireless technology is protected from unauthorized

disclosure and that the introduction of Wireless Local Area Networks (WLANs) into the DoD environment protects DoD networks from unauthorized access and other malicious attacks.

2 POLICY

It is MHS Policy that:

- 2.1 This policy applies to all MHS data transmitted via a wireless connection except as noted below.
 - a. Examples of MHS data include, but are not limited to the following: official e-mail transmissions; SI/PHI/data covered under the Privacy Act; data designated as “Unclassified/For Official Use Only;” and procurement of SI. This includes data transmitted wirelessly to and from medical devices (e.g., handheld order-entry devices, medical monitoring devices, Portable Electronic Devices (PEDs), Personal Digital Assistants (PDAs)).
 - b. Wireless connections typically include, but are not limited to, the 802.11 Institute of Electrical and Electronics Engineers Standard for WLANs.
 - c. Bluetooth devices shall not be used to store, process, or transmit DoD information unless Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules,” dated December 3, 2002
 - d. compliant cryptographic modules are used to encrypt the data during transmission.
 - e. The MHS Wireless Policy does not apply to wireless transmissions to or from receive-only pagers, Global Positioning System (GPS) receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems. The detection segment of a PED (e.g., the laser beam between a laser disk and its reader head; between a barcode and a scanner head; or radio frequency (RF) energy between wireless identification tags, both active and passive, and the reader/interrogator) does not require encryption.
- 2.2 This document should be used in conjunction with policy, directives, and Information Assurance (IA) measures for wireless implementations from the DoD, DISA, National Security Agency (NSA), the Services, and MHS to protect data on wireless Local Area Networks (LANs) and portable devices.

Acquisitions for new and/or upgraded equipment used for the transmission of MHS data utilizing 802.11 wireless technology using Defense Health Program (DHP) funds must meet the minimum requirements outlined in this document.

Additional publications are listed in Appendix A of the DISA Security Technical Implementation Guide (STIG) regarding wireless policies, guidance, standards and vulnerabilities, and Wired Equivalency Privacy (WEP) vulnerabilities.

- a. References (a), (b), and (c) identify the minimal implementation requirements of wireless technologies for the transmission of information on DoD networks. These references provide guidance for two categories of wireless device usage. The WLAN Technology section discusses wireless networking technologies and associated security

policies. The Remote Wireless Networking Technologies section discusses remote access devices, such as mobile telephones and personal data devices, two-way pagers, and e-mail devices.

- b. Wireless devices and systems that do not meet the security requirements of references (d) and (e) should not be used to store, process, access, or transmit DoD information unless approved by the Designated Approving Authority (DAA) as necessary to meet specific mission requirements.
 - c. The Site DAA shall ensure that DoD, MHS, and Service-specific guidance regarding implementation of wireless infrastructure, transport, and storage of PII/PHI data are followed. The site DAA shall ensure procedures are developed and followed for safe implementation, intrusion detection, and monitoring of wireless technologies. See reference (f) for additional recommendations and industry best practices for the mitigation of wireless risks.
- 2.3 Data Encryption. Encryption of data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the DAA. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS Pub 140-2 Overall Level 1 or 2.
- 2.4 Wireless transmission of classified information is prohibited.
- 2.5 Lost or Stolen Devices with Wireless Capability. The loss or theft of any device with wireless capability should be immediately reported to the Information Assurance Officer (IAO) or designated individual. Remote network access by the device should be immediately deactivated upon notification of the device reported as lost or stolen
- 2.6 Disruption and Interference. All newly deployed wireless technologies must satisfy all existing standards as required by DoD, federal, and local Service policy, with particular attention for medical, safety, and emergency devices.
- 2.7 User Training Program
- a. Ensure that users on the network are fully trained in computer security awareness, HIPAA privacy and security, and the risks associated with wireless technology.
 - b. Ensure that visitors to the site are made aware of wireless device usage and wireless transmission of data.
- 2.8 Intrusion Detection. Implementation of a fully automated wireless rogue detection system is strongly recommended.
- 2.9 Wireless technology implementation integrated or connected to MHS networks are considered part of those networks, and must comply with DoD Directive 8500.1 and be certified and accredited in accordance with DoD Instruction (DoDI) 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," dated December 30, 1997.
- 2.10 Wireless technologies for transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA, in consultation with a Certified TEMPEST Technical Authority (CTTA). The

responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

- 2.11 Introduction of wireless communications for the transmission of MHS data can have a significant adverse effect on the security posture of the information system (IS). A security review and documentation should be conducted in accordance with DoDI 5200.40 and the HIPAA Security Rule.
- 2.12 Transfer of data via infrared ports should be avoided where possible to minimize inappropriate access to MHS data. Protected methods of data transfer should be utilized when feasible. If transfer of MHS data via infrared is required, the infrared ports should be adjacent to each other for the duration of the transmission.
- 2.13 Preventive measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources, such as microwave ovens.
- 2.14 Active screening for wireless devices shall be conducted to detect/prevent unauthorized access of TMA Component information.

3 PROCEDURES

Wireless network devices extend network accessibility by reducing the requirements of the physical infrastructure needed in the traditional wired network. Vulnerabilities of wired networks apply to wireless ones as well. However, the unique properties of the wireless network introduce several vulnerabilities that warrant additional security analysis. Removing the traditional physical constraints of wired networks makes intrusion detection more difficult, and makes eavesdropping and denial of service attacks potentially easier.

Since wireless signals are radio transmissions, they can be intercepted by radio receiving devices, even devices outside of the intended service area. If data transmissions are not adequately protected, the intercepted data can be read and understood in a matter of seconds.

Wireless transmissions circumvent traditional perimeter firewalls. Technological advances in wireless signaling may increase transmission distances, further increasing the problem of unauthorized reception. Improper implementation of a wireless network may allow an unauthorized user access to wired networks and the data and assets residing on it. Without appropriate IA measures, DoD networks are faced with the potential of growing numbers of unauthorized users looking for rogue access points.

Differences between protocols in the 802.11 family are not significant with respect to security. The 802.11 WLANs all use the same layer 2 packets; the difference is in the physical layer.

Attacks on WLANs have become more prevalent and easier with the wide array of publicly available tools. This situation emphasizes the need for secure implementation of wireless technologies and constant vigilance against intrusion related activities from unauthorized sources.

- 3.1 Protection and mitigation strategies for MHS data during transmission via wireless 802.11x LAN technologies, regardless of transmission method, should include:

- a. Data in transit via traditional wired Wide Area Networks/Metropolitan Area Networks/Local Area Networks (WAN/MAN/LAN)
 - b. Data at rest:
 - Stored on portable devices (e.g., laptops, Blackberry™ devices).
 - Stored on workstations.
 - Stored on application storage devices.
 - c. Authentication and access control procedures for networks, applications and portable devices
 - Password and encryption protection mechanisms.
 - Logon passwords.
 - Timed log-out features.
 - d. HIPAA-related concerns
 - Audit requirements.
 - HIPAA security awareness training.
 - the Information Assurance Manager (IAM) roles and responsibilities.
 - e. Disposal of data storage and portable devices
- 3.2 The primary areas of concern for mitigation of security risks when incorporating a wireless solution into a wired network include, but are not limited to:
- a. Internal Threats
 - Unauthorized undetected access.
 - Accidental association to neighboring networks.
 - Insecure configurations.
 1. Default passwords.
 2. Weak encryption.
 3. Weak authentication.
 4. Broadcasting of service set identifier (SSID).
 5. Lost or stolen devices.
 6. Media access control (MAC) spoofing.
 - b. External Threats
 - Scanning, snooping, and probing.
 - WEP and extensible authentication protocol (EAP) attacks.
 - MAC spoofing.
 - AP association attacks.
 - Redirection attacks.

- Denial of Service (DoS) attacks.
- Springboard attacks.

3.3 MHS Chief Information Officer (CIO) shall:

- a. Provide oversight guidance for wireless transmissions of MHS data.
- b. Provide analytical and standards support to the TMA Components concerning proper employment of wireless technologies.

3.4 DAAs or the designated representatives shall:

- a. Ensure that all new commercial wireless procurements comply immediately with the provisions of this guide.
 - b. Implement accountability, access control, and audit trail methods to track and actively monitor wireless transmissions of MHS data. The type of transmission authorized and associated network utilized for all TMA Component communications must be identified and documented.
 - c. In accordance with the DoD Information Technology Security and Accreditation Process (DITSCAP):
 - Control wireless transmissions of MHS IS data under their cognizance to ensure the wireless solutions (including external interfaces to commercial wireless services) do not introduce vulnerabilities undermining the assurance of the other interconnected systems.
 - Ensure wireless interfaces are consistent with federal, DoD, and local Service policies.
 - d. Ensure wireless Personal Area Networks (PANs) (e.g., Bluetooth™) capabilities are removed or physically disabled from a device unless FIPS Pub 140-2 validated cryptographic modules are implemented.
 - e. Promote the use of wireless KM processes when evaluating potential wireless solutions.
 - f. Develop a local Wireless Device Usage Statement specific to their activity for End-users. (See Attachment 1 for a sample statement.)
 - g. Provide initial and ongoing security training specifying precautions for use of wireless communications.
- 3.5 Users shall:
- a. Adhere to MHS and local Service policy for wireless devices.
 - b. Immediately report to IAM any suspected compromise of MHS data transmissions.
 - c. Sign a Wireless Device Usage Statement specific to the local activity signifying an understanding of the procedures and policies for wireless devices.

4 REFERENCES

- a. DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004
- b. Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG), Version 2, Release 1, July 10, 2003¹
- c. Defense Information Systems Agency (DISA) "Wireless Security Checklist," Version 2, Release 1.1, July 30, 2003²
- d. DoDD 8500.1, "Information Assurance (IA)," October 24, 2002
- e. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- f. National Institute of Standards and Technology (NIST) Special Publication 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," November 2002³
- g. DoDD 8100.1, "Global Information Grid Overarching Policy," September 19, 2002
- h. DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (supplemented by DoD 8510.01-M, Applications Manual, July 2000)
- i. FIPS Publication 140-2, "Security Requirements for Cryptographic Modules," December 3, 2002
- j. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996
- k. Privacy Act of 1974 (5 US Code Sec. 552a)
- l. DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003
- m. "Military Health System Information Assurance Policy Guidance," March 5, 2004

¹ Available at <https://iase.disa.mil/techguid/stig/wireless-stig-v1r4-010903.doc>

² Available at <https://iase.disa.mil/techguid/checklist/wireless-chklstv2r11-073003.doc>

³ Available at http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

5 ACRONYMS

CIO.....	Chief Information Officer
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DHP.....	Defense Health Program
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DoD.....	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoS	Denial of Service
EAP.....	Extensible Authentication Protocol
FIPS.....	Federal Information Processing Standard
GIG	Global Information Grid
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IAM.....	Information Assurance Manager
IAO	Information Assurance Officer
IP	Internet Protocol
IS.....	Information System
JMISO.....	Joint Medical Information Systems Office
KM	Knowledge Management
LAN	Local Area Network
MAC	Media Access Control
MHS	Military Health System
NIST.....	National Institute of Standards and Technology
NSA.....	National Security Agency
PAN.....	Personal Area Network
PDA.....	Personal Digital Assistant

PED.....Portable Electronic Device
PEO.....Program Executive Office
PHI.....Protected Health Information
PII.....Personal Identifiable Information
RF.....Radio Frequency
SI.....Sensitive Information
SSID.....Service Set Identifier
STIG.....Security Technical Implementation Guide
TMA.....TRICARE Management Activity
TRO.....TRICARE Regional Offices
WEP.....Wired Equivalency Privacy
WLAN.....Wireless Local Area Network

WIRELESS DEVICE USAGE STATEMENT

Wireless Device Information

1. Manufacturer: _____ Model: _____ Serial Number: _____
2. Software Installed on Wireless Device: _____
3. Department where Wireless Device will be located/used: _____
4. Local Area Network System to be connected to: _____
5. Property Account Number of CPU or designated server on which wireless device software will be installed:

Wireless Device Usage

1. Wireless Devices:
 - a. Shall be secured when not in use.
 - b. Shall only be connected to the identified Local Area Network listed above.
 - c. Shall conform to DoD policies of operation for information systems.
 - d. May be used to carry information from a desktop workstation, including schedules, contact information, notes, and e-mail items from Microsoft Outlook.
 - e. May be used to take notes, save information, or write e-mails while away from Wireless Device user's desk.
 - f. May be used to synchronize information with the Wireless Device user's desktop workstation using direct connect cables.
2. Wireless devices shall NOT be:
 - a. Used to process or store classified information.
 - b. Connected to any classified information system or network.
 - c. Used with modems to exchange information with wireless device user's desktop or other systems on the network.
 - d. Used to synchronize any equipment features or devices across any network.
 - e. Used to download and install freeware or shareware software enhancements to wireless devices. Such software is from untrusted sources and may contain malicious code.
 - f. Used for storing, processing or transmitting SI or PHI without explicit written approval of the DAA
 - g. Left unattended while attached to a government information system.
3. Please contact your Information Assurance Manager (IAM) if you have any questions or require additional information.

Wireless Device Use Agreement

1. I have read and understand the security guidelines for wireless device usage.
2. I understand the necessity for safeguarding my Wireless Device and recognize the requirement for maintaining confidentiality of all data stored in it.
3. I agree to abide by the Wireless Device Usage statements above and understand that failure to comply shall result in the loss of my wireless device use privilege.
4. I agree to abide by the Privacy Act of 1974 (5 U.S.C. 552a) that requires federal agencies to safeguard personal data processed by and stored on wireless devices or technologies.
5. I agree to abide by the Health Insurance and Portability Accountability Act of 1996 (PL 104-191) and the DoD 6025.18-R Health Information Privacy Regulation.
6. I shall immediately contact my IAM if I suspect a compromise of the device, the data it contains, or the transmission of data to or from the device.

IAM Information	User Information
Name: Title: Date: Signature:	Name: Title: Date: Signature: