Department of Veterans Affairs
Washington, DC 20420

VA Directive 6550
Transmittal Sheet
September 5, 2007

PRE-PROCUREMENT ASSESSMENT FOR MEDICAL DEVICES

1. REASON FOR ISSUE: To establish the policy requirements for assessment by facility technical support services for medical devices that will be connected to VA information networks and/or contains patient information before procurement action.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive requires that pre-procurement assessments be conducted to assure that these medical devices are integrated with VA information technology networks and systems effectively and securely.

3. RESPONSIBLE OFFICE: The Office of Information and Technology (OI&T), 810 Vermont Avenue, NW, Washington, DC 20420, is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None

5. RESCISSION: None.

Certified By:

/s/

Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Robert T. Howard
Assistant Secretary for
Information and Technology

Distribution: Electronic

PRE-PROCUREMENT ASSESSMENT FOR MEDICAL DEVICES

1. PURPOSE AND SCOPE:

a. This Office of Information and Technology (OI&T) Directive establishes the requirement for assessment by facility technical support services for medical devices that will be connected to VA information networks and/or contains patient information before procurement action.

b. Increasingly, sophisticated medical devices are designed with the added capability to store patient data and be networked to facility information technology networks. There are many benefits when medical devices are networked including ready availability of data and images from diagnostic exams to clinical staff nearly as soon as they are released, thereby providing for more effective care. But the increasing use of networked technology also means increased bandwidth competition on facility information networks, in addition to increased exposure to risk for medical devices that are now communicating over the same networks exposed to software attacks. Even for devices that are not networked, storage of patient data on the device creates the possibility of loss of patient data. Including the appropriate technical service assessment during the acquisition planning process will address both risk and provide a more effective integration into hospital operations. Key technical services includes Information Technology, Information Security and Biomedical Engineering who all have an important role assuring VA continues to maintain a safe and secure environment for the medical center patient data.

2. POLICY: Quality Assurance and maintenance activities compliant with the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) requirements for all medical devices are assigned to the VHA Biomedical Engineering program. An additional requirement for pre-procurement assessment is necessary for networked medical devices and devices with the ability to store patient information. Pre-procurement assessment is conducted to assure that these medical devices are integrated with VA information technology networks and systems effectively and securely.

3. RESPONSIBILITIES: Risk analysis is conducted using the provided device information worksheet by the facility Biomedical Engineering staff, facility Office of Information and Technology Enterprise Field Operations staff, and the facility Information Security Officer.

a. Network Directors. Network Directors are responsible for:

(1) Developing VISN-wide policy and procedures to implement the requirements of this directive.

(2) Assuring policy and procedures are developed with input from Biomedical Engineering, Information Technology and Information Security.

(3) A Sample checklist of pre-procurement assessment and pre-implementation items are included in Attachments A and B of this Directive. At a minimum, assessment will address network requirements, remote access, data security, systems integration requirements, IT support and upgrade requirements and the Manufacturer Disclosure Statement for Medical Device Security (MDS^2).

b. Facility Directors. Facility Directors are responsible for:

(1) Assuring completion of pre-procurement assessment consistent with VISN wide policy and procedures for networked and stand alone medical devices that store electronic protected health information (ePHI).

(2) Reviewing risk analysis and authorizing acquisition and installation of medical devices in accordance with the review and concurrence requirements listed in this directive.

c. Enterprise Operations and Infrastructure. OI&T Enterprise Field Operations

(1) Review and concur in the acquisition of each medical device from an IT operations, integration, and technical perspective and ensuring the acquisition is entered into the IT Tracker system as an approved acquisition action.

(2) Configuring the Medical Device VLAN to appropriately segment the medical device from the production network.

(3) Entering the device into the networked medical device VLAN inventory.

(4) Providing consultation on network configuration and possible additional security precautions to protect the device and the network from malware.

(5) Reviewing and concurring with all necessary medical devices IT related operations, integration, and ongoing IT upgrades and support documentation is complete and that necessary specific roles and accountabilities are identified.

(6) Newly identified unique IT technical requirements that do not meet current IT engineering standards will be forwarded to Enterprise Infrastructure Engineering for review and concurrence.

d. Biomedical Engineering. Biomedical Engineering is responsible for the following:

(1) Obtaining Manufacturer Disclosure Statement for Medical Device Security.

(2) In conjunction with the manufacturer/vendor, completing the pre-procurement and pre-implementation worksheets.

(3) Identify other devices and systems requiring communication for proper operation

(4) Maintaining an accurate inventory of medical devices

(5) Assuring a quality assurance program is designed for the useful life of the device, consistent with statutory and regulatory requirements including FDA, NFPA and JCAHO.

(6) Engaging with local IT in the development of RFPs and SOWs to ensure possible IT needs are identified and input is provided.

e. Information Security Officers. Information Security Officers are responsible for:

(1) Reviewing and concurring in each acquisition of a medical device from an information security perspective.

(2) Determining whether the equipment manufacturer has an existing Business Associate Agreement (BAA) with VHA, and assisting with establishing a BAA where needed.

(3) Determining the current status of VPN access for the manufacturer's service organization, and assisting with establishing remote access where necessary through accepted VA procedures.

(4) Coordinate with the Office of Field Operations and Security to ensure access to the latest security guidance addressing federal requirements and VA Policies and Directives.

Medical Equipment Pre-Implementation Worksheet

1. For networked medical devices and medical devices storing ePHI, utilize the Medical Equipment Evaluation Matrix below to determine the assessment/documentation requirements.

2. Where indicated, obtain a Manufacturer Disclosure Statement for Medical Device Security (MDS[2)] Form from the equipment manufacturer. This document covers most pertinent information related to networking and risk exposure for medical devices. http://www.himss.org/content/files/MDS2FormInstructions.pdf

3. Complete the Medical Device Pre-Procurement Assessment (PPA) as required.

4. Once required concurrences are obtained, notify procurement that the equipment is ready for purchase.

5. In conjunction with the facility ISO and OI&T Field Ops, develop implementation, support, and upgrade, remediation plans including roles and responsibilities based on the attached Pre-Implementation Worksheet or additionally acquired documentation.

Medical Equipment Evaluation Matrix

CONNECTIVITY➔ / **STORAGE⬇**	**1**	**2**	**3**
A	N/A	PPA	PPA
B	MDS[2]	MDS[2] & PPA	MDS[2] & PPA
C	N/A	MDS[2] & PPA	MDS[2] & PPA

CONNECTIVITY:
1 = Stand Alone Device, Computer Based
2 = Network Connected Device, Replacement or additional with similar infrastructure impacts
3 = Network Connected Device, New Device

STORAGE:
A = Does Not Store ePHI
B = Short Term ePHI Storage/Input of Results into CPRS
C = Long Term ePHI Storage Repository

Medical Equipment Pre-Procurement Assessment
(to be completed by potential vendors)

Equipment Description: _____

Vendor/Model: _____

Vendor Contact: _____

Requesting Clinical Service: _____

Medical Equipment Configuration

- ☐ What OS does the system utilize? _____
- ☐ Can critical security patches be installed without prior vendor approval? ☐ YES ☐ NO
- ☐ Does the device incorporate a switch or hub into its design? ☐ YES ☐ NO
- ☐ Is the switch or hub required as part of the system configuration? ☐ YES ☐ NO
- ☐ Which Anti-virus software is approved by the device manufacturer? _____
- ☐ If server based, does the system require a specific version of Java for proper client operation? ☐ YES ☐ NO
- ☐ If server based, does the system utilize an ActiveX control for client interaction? ☐ YES ☐ NO
- ☐ If yes, specify configuration requirements.

Authentication and User Accounts

- ☐ Is an administrator or power user account required to operate the device? ☐ YES ☐ NO
- ☐ Is an administrator account required for service? ☐ YES ☐ NO
- ☐ Can the device be made to require user authentication? ☐ YES ☐ NO
- ☐ Does user authentication support Strong Passwords? ☐ YES ☐ NO
- ☐ Does user authentication support password aging? ☐ YES ☐ NO
- ☐ Can the device be part of the facility's Windows domain? ☐ YES ☐ NO

Data Handling

- ☐ Will the medical device require data backups? ☐ YES ☐ NO
- ☐ Is ePHI stored only on a drive partition to assist with end of service media sanitization? ☐ YES ☐ NO
- ☐ What ePHI data elements are stored on the device? _____
- ☐ Can ePHI be stored directly to a network drive, rather than local (machine) storage? ☐ YES ☐ NO

Networking

- ☐ What are the LAN/WAN bandwidth requirements for full connectivity/performance? _____
- ☐ What ports in the TCP/IP stack are utilized for network communication? _____
- ☐ Can unutilized ports be closed without negatively impacting device operation? ☐ YES ☐ NO
- ☐ Can the device support DHCP for network address configuration? ☐ YES ☐ NO
- ☐ How many IP addresses does the device require? _____
- ☐ Can the device operate properly without connection to the Internet? ☐ YES ☐ NO
- ☐ Can the target system be addressed via a fully qualified domain name (FQDN)? ☐ YES ☐ NO

Wireless

- ☐ Does the device utilize wireless communication? ☐ YES ☐ NO
- ☐ If so, what protocols are used? _____
- ☐ Is any ePHI transmitted via the wireless link? ☐ YES ☐ NO
- ☐ Does the device support installation of FIPS 140-2 certified wireless security clients? ☐ YES ☐ NO
- ☐ If so, which ones?

Integration with VA Health Care Information Systems

☐	Has the device been validated with VA's Clinical Procedures package?	☐ YES	☐ NO
☐	Has the device been validated with VA's Vista Imaging?	☐ YES	☐ NO
☐	Does the device have a bi-directional HL7 interface?	☐ YES	☐ NO
☐	Provide a DICOM conformance statement.	☐ YES	☐ NO

(to be converted to a VA form)

Medical Equipment Pre-Implementation Worksheet

Equipment Description:

Vendor/Model:

Vendor Contact:

Requesting Clinical Service:

Contact Information & Sign-Off

Clinical Service POC: Phone:

Biomedical Engineering POC: Phone:

ISO: Phone:

IT POC: Phone:

Medical Equipment Documentation Review

- ☐ Manufacturer Disclosure Statement for Medical Device Security (MDS^2)
- ☐ Existing Site-to-Site or One-VA VPN Agreement
- ☐ Purchase documents and associated equipment quotations
- ☐ Business Associate Agreement
- ☐ Equipment description, information flow, and network connectivity requirements
- ☐ Documentation of network configuration and installation requirements
- ☐ Clinical Procedures integration documentation provided with VA contacts, if applicable
- ☐ DICOM conformance statement provide, if applicable

Security Precautions

- ☐ Does the equipment support Anti-virus protection with updates via McAfee ePolicy Orchestrator? ☐ YES ☐ NO
- ☐ Does the equipment support automated OS critical patch installation? ☐ YES ☐ NO
- ☐ Will the medical equipment be configured for Device Authentication using Active Directory? ☐ YES ☐ NO
- ☐ Will the medical equipment be configured for User Authentication using Active Directory? ☐ YES ☐ NO
- ☐ Who will provide and manage: Disaster Recovery?
- ☐ Will vendor require Remote Access via VPN? ☐ YES ☐ NO
- ☐ Will vendor provide a network device (switch, router)? Needs risk assessment. ☐ YES ☐ NO
- ☐ Will vendor provide any wireless devices? Needs risk assessment. ☐ YES ☐ NO

Network Design and Constraints

- ☐ Notification to network administrator to configure medical VLAN Medical VLAN:
- ☐ Medical equipment installation location(s)
- ☐ Network administrator reviews risk assessment for any network or wireless devices.
- ☐ List all target systems that the device will communicate with
- ☐ Network administrator configures the ACL with input from Biomedical Engineering, verifies connectivity, and documents configuration.

Post Installation Support Strategy

☐ Post implementation support strategy developed.
☐ Post implementation secure use strategy developed.(i.e. frequency of removal of ePHI from device, physical security of device, etc.)

(to be converted to a VA form)