Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6550
Transmittal Sheet
February 20, 2015

PRE-PROCUREMENT ASSESSMENT FOR MEDICAL DEVICE/SYSTEMS

1. REASON FOR ISSUE. This Department of Veterans Affairs (VA) Directive establishes the technical pre-procurement assessment (PPA) requirements for medical devices/systems, including medical devices/systems that are connected to the VA information networks and medical devices that store sensitive patient information.

2. SUMMARY OF CONTENTS/MAJOR CHANGES. Major changes include the updating of mandatory policy, responsibilities, and definitions. This policy references The Joint Commission (TJC) standards pertaining to selection of medical equipment. The policy identifies Contracting responsibilities. It clarifies IT Acquisition Request System (ITARS) requirements specific to medical devices/systems. This policy separates the PPA from implementation planning requirements. The industry standard Manufacturer Disclosure Statement for Medical Device Security (MDS2) form previously required under this policy will be included in a separate policy covering implementation planning requirements.

3. RESPONSIBLE OFFICE. Veterans Health Administration (VHA) Office of Healthcare Technology Management (10NA9) is responsible for the material contained in this Directive.

4. RELATED DIRECTIVE/HANDBOOK. VA Directive 6500, VA Handbook 6500, The Joint Commission Environment of Care Standard EC.02.04.01 EP1.

5. RESCISSION. VA Directive 6550, September 5, 2007, is rescinded.

CERTIFIED BY:

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer
for Office of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer
for Office of Information and Technology

Distribution: Electronic Only

PRE-PROCUREMENT ASSESSMENT FOR MEDICAL DEVICE/SYSTEMS

1. PURPOSE:

This Department of Veterans Affairs (VA) Directive establishes the technical PPA requirements for medical devices and medical systems, especially medical devices and systems that are connected to the VA information networks and medical devices that store sensitive patient information.

2. BACKGROUND:

a. All medical devices/systems are assessed for a variety of factors prior to procurement and during the acquisition process. These factors include, but are not limited to, establishing technical requirements to support intended clinical use, human factors engineering, reliability, safety, integration, and available space and utilities. The Joint Commission standards state “The hospital solicits input from individuals who operate and service equipment when it selects and acquires medical equipment.” VHA Biomedical Engineering facilitates input and requirements definition from clinical and technical staff and provides technical input to the equipment selection process. Biomedical Engineering is responsible for ensuring that medical equipment purchases are reviewed by the appropriate parties. Biomedical Engineers at medical facilities and Veterans Integrated Service Networks (VISN) coordinate with the Facility or VISN Chief Information Officer (CIO) to ensure that thorough technical assessment is conducted prior to acquisition of medical devices/systems. The Facility or VISN CIO is responsible for identifying and involving appropriate offices within the Office of Information Technology (OIT), including within the Information Security (ISO) organization, whether locally, regionally, or nationally-based, which should provide input to ensure that the medical equipment under review can be operated as intended in the medical facility.

b. Increasingly, medical devices are designed with the capability to store patient data and to be connected to facility data networks. There are many benefits when medical devices are networked, including availability of patient data and diagnostic images for clinical staff, thereby providing for more timely and effective care. However, use of networked medical technology leads to increased bandwidth competition on facility data networks, increased risk for medical device exposure to malware, system integration challenges, and growth in data storage requirements. Storage of sensitive patient data on medical devices creates the possibility of patient data loss.

c. Evaluating the configuration and security profile of medical devices during the acquisition planning process will identify potential risks and ultimately provide for more effective and safe integration of medical devices into hospital operations. Key organizations involved in this process are: Biomedical Engineering, Information Technology, Information Security, and Contracting. All of the aforementioned disciplines have important roles in ensuring that VA maintains an environment that supports safe and secure operation of medical devices.

d. Within this document, a medical device/system is defined as any device or system that meets any of the following requirements:

(1) Used in patient healthcare for diagnosis, treatment (therapeutic), or physiological monitoring of patients. This includes server-based medical equipment and clinical systems. Examples of medical devices/systems include, but are not limited to, physiological monitoring systems, ventilators, infusion pumps, Computed Tomography (CT) scanners, MUSE cardiology information system, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS), and laboratory analyzers. Medical devices directly connect to the patient; process human and other biologic specimens; create medical images, display electrophysiological waveforms; obtain physiologic measurements, or directly perform therapeutic-support to the patient.

(2) The device/system has gone through the Food and Drug Administration's (FDA) Premarket Review or 510k Process.

(3) Is incorporated as part of a medical device system in such a fashion that if modified, the device or system component could have a negative impact on the functionality or safety of the main medical device/system.

3. POLICY:

a. To ensure compliance with TJC requirements, VHA has assigned responsibility for life cycle management of medical devices and medical systems to the VHA Office of Healthcare Technology Management (10NA9) and field operations-based Biomedical Engineering programs. Biomedical Engineering shall lead the technical requirements definition and related PPA processes for all medical devices/systems as an integral aspect of medical technology lifecycle management to manage risks and to help ensure a safe Environment of Care. Biomedical Engineering will coordinate technical PPA with the VA OIT for medical devices/system that will be connected to the VA data network or store sensitive patient data to ensure requirements for information protection, IT infrastructure capacity, and medical device security are jointly addressed.

b. PPAs shall be conducted for medical devices/systems that will be connected to VA information networks or medical devices that store sensitive patient information to ensure that medical devices/system are safely and securely integrated with VA's clinical and IT systems and networks. Biomedical Engineering shall lead the PPA process, ensuring that input from OIT is received prior to purchase. Biomedical Engineering shall confer with medical staff and equipment users regarding clinical requirements. VISNs and medical facilities will utilize Appendix A to complete and document the PPA. Specific procedures are described in Appendix B.

c. Implementation planning is a separate and distinct process from PPA and involves obtaining the MDS2 and submitting the Medical Device Isolation Architecture Virtual Local Area Network (MDIA VLAN) change request(s). Implementation planning activities shall occur prior to equipment delivery and shall be jointly coordinated by

Biomedical Engineering, OIT, Information Security, Facilities Engineering, the requesting Clinical Service(s), Clinical Informatics (as required), and the medical equipment contractor. Biomedical Engineering (BME) is responsible to lead, or co-lead with clinical departments, the implementation planning for medical devices/systems.

d. The PPA serves as the multi-disciplinary (BME, OIT and ISO) technical review and approval process for network connected medical device/system procurement. As such, IT Tracker Number (ITARs) approval for this subset of procurements would be a duplicative process and is not required for medical devices/systems purchases. In instances where medical equipment or medical system components are procured off contract vehicles, such as Solutions for Enterprise Wide Procurement (SEWP), that require an ITARS number, “6550” will be used as the default number.

e. For procurements of identical medical equipment items requiring a PPA, only one assessment need be completed. For subsequent procurements of the same medical equipment, an additional PPA is required to ensure sufficient OIT infrastructure is available in the required timeframe and no other critical IT environment changes have since the initial approval. However, if a subsequent procurement of the same medical equipment occurs within one (1) year of an assessment and there are no changes to the equipment, then submission of an additional PPA form is not required. For server based medical systems, separate PPAs are required for the server infrastructure and client devices.

4. RESPONSIBILITIES:

a. **Network Directors.**

Network Directors are responsible for:

(1) Ensuring facilities in their Network have policies and procedures in place to implement the requirements of this Directive. Ensure that consolidated medical equipment acquisitions and VISN-level medical system acquisitions meet the requirements of this Directive including the utilization of Appendix A to complete the PPA

(2) Ensuring that the policies and procedures are developed with input from Biomedical Engineering, OIT, and Information Security at the facility and VISN level.

b. **Facility Directors.**

Facility Directors are responsible for:

(1) Developing local facility policy and procedures that meet the intent of this Directive.

(2) Ensuring that the local PPA is consistent with policy and procedures for networked medical devices and medical devices that store sensitive patient data.

(3) Ensuring that every effort is made by Biomedical Engineering, OIT, and the ISO to reach consensus on medical device PPA review. For any items where outstanding issues remain that cannot be resolved by the Biomedical Engineering and OIT, the Facility Director, as the designated Medical Device/System Owner will review the risk analysis and make a risk-based decision to authorize or reject the acquisition. The risk–based decision shall consider clinical benefit to patient care on balance with projected technical and/or security risks. Documentation of the risk-based decision shall be signed by the Medical Center Director and kept on record with Biomedical Engineering. These instances are expected to be extremely rare as every effort should be made to resolve technical risk issues in context of clinical capabilities before escalating to the Medical Center Director.

c. **Biomedical Engineering.**

Biomedical Engineering staff is responsible for:

(1) Ensuring a quality assurance and life cycle management program is designed and implemented for all medical devices and medical systems, consistent with statutory and regulatory requirements including but not limited to FDA, National Fire Protection Agency (NFPA), TJC, VA policy and procedures, technical infrastructure, and cybersecurity risk management.

(2) Lead, or co-lead with clinical departments, the implementation planning for medical devices/systems

(3) Engaging with medical and clinical staff, local OIT staff, and Contracting personnel in the development of applicable statements of work (SOWs), requests for proposals (RFPs), disaster recovery and pre-procurement planning to ensure incorporation of applicable technical and architectural standards, IT capacity, and information security considerations.

(4) Identifying interconnectivity requirements of the medical device and providing OIT staff with network communication and configuration information required to connect the device to a MDIA VLAN.

(5) Ensuring that maintenance requirements for hardware and software are accounted for in pre-purchase planning and discussed with OIT staff upon request.

(6) In coordination with Contracting, ensuring that vendors provide documentation required for procurement, implementation, integration, configuration, and sustainment of medical equipment.

(7) Completing the PPA in collaboration with OIT and in conjunction with the manufacturer/vendor(s).

(8) Completing VA Handbook 6500.6 Appendix A for acquisition of medical equipment.

(9) Maintaining completed copies of PPA and other relevant documents on file throughout the life of the medical device/system.

(10) Updating the medical device inventory database and networked medical device inventory coinciding with the procurement, modification, or decommissioning of the medical device, to assure inventory accuracy.

(11) Ensuring that medical devices and systems being procured are aligned with existing VHA national standards, as appropriate and relevant (e.g. Surgical Robotic Systems).

d. **Facility CIOs (Network CIOs for VISN-wide procurements).**

CIOs are responsible for:

(1) Engaging proactively with Biomedical Engineering in the development of RFPs, SOWs, disaster recovery, and pre-procurement planning to ensure IT requirements are identified.

(2) Seeking engagement with appropriate members of OIT at the local, regional, and national level for coordination and approval for desired medical equipment.

(3) Providing consultation on network configuration and in coordination with the ISO, pertinent security precautions to protect the device and the network from malware.

(4) Reviewing and concurring with the acquisition of data network connected medical devices from an IT capacity and operations, integration, and technical perspective.

(5) Reviewing and concurring with all necessary medical device IT-related operations and integration requirements.

(6) Ensuring that OIT support roles and responsibilities are identified. Providing network and physical access and OIT infrastructure services as needed for the operation of the network-connected medical device, to the extent that approved resources permit.

e. **Information Security Officers.**

ISOs are responsible for:

(1) Engaging proactively with Biomedical Engineering in the development of RFPs, SOWs, disaster recovery, and pre-procurement planning to ensure security requirements are identified.

(2) Providing remote access capabilities for the servicing vendor when necessary, through proper VA account establishment procedures.

(3) Coordinating with the Office of Field Security Services (FSS) and FSS Health Information Security Division (HISD) to ensure responsible parties have access to the latest VA security policies.

(4) Reviewing VA Handbook 6500.6 Appendix A for procurements that involve sensitive information.

(5) Determining whether the equipment manufacturer has an existing Business Associate Agreement (BAA) with VHA (http://vaww.va.gov/hia/signedbaa1.htm) and initiating a new BAA request where needed.

(6) Determining whether the equipment manufacturer has an existing Memo of Understanding-Information Security Agreement (MOU-ISA) with VHA and initiating a new MOU-ISA request where needed.

f. **Contracting Officers.**

Contracting Officers are responsible for:

(1) Engaging proactively with Biomedical Engineering and medical equipment Integrated Product Teams (IPT) in the development of SOWs, RFPs, and other acquisition/procurement documents to meet pre-procurement technical and security risk management requirements for all medical devices/systems.

(2) Ensure that Biomedical Engineering was properly engaged in the procurement of all medical devices by including a signed copy of the 6550 Appendix A when applicable.

(3) Documenting in the contract files that OIT was properly and meaningfully engaged in procurement of all network connected medical devices/systems.

VA Medical Equipment Pre-Procurement Assessment

(*Indicates field is completed by Biomedical Engineering)

*Equipment Category (VA-MDNS): Postage Machines	*Vendor:
*Requesting Service:	*Model:
*Requestor:	Vendor Contact:
*Installation Location: (Room-Bldg-Division):	If server based, specify rack space and power requirements:
*Biomedical Engineering Point of Contact:	*MDIA VLAN Number for Installation:
*Equipment Description (i.e., layman's description of equipment function and systems it communicates with): Postage stam and mailing machine with letter Inserter used for folding, inserting and sealing envelpoes. The postage portion of the system will download all informaon for processing reports on amoun t of postage used, type of postage used i.e. certified, priority, etc.	
*If Biomedical Engineering is NOT the Primary System Manager for system management and maintenance, please note the responsible department below. Other	

Medical Device /System Configuration

What OS and version/Service Pack does the system utilize (e.g., Win7- SP1, Win Svr 2008, Linux)?	
Does the system use a database application to operate?	☐ Yes ☑ No
If yes, specify which application/version:	
Membership in the facility's Windows Domain is: ○ Required ○ Recommended ○ Not Recommended ◉ N/A	
Is a desktop web browser required to access the medical system/application?	☐ Yes ☑ No
If yes, specify which browsers and versions are supported: If yes, does it require the use of https: and the VA SSL certificates – explain below:	
If a browser is required, does it require a specific version of Java?	☐ Yes ☑ No
If yes, specify the version:	
Is ActiveX required for client operation?	☐ Yes ☑ No
If yes, specify configuration requirements:	
If Windows based, can the system use the National Medical Device Update Server for OS patches?	☐ Yes ☐ No
If no, specify how OS patching will be accomplished:	
Can critical and routine OS and system security patches be applied as they become available without prior vendor approval?	☐ Yes ☑ No
If no, specify how approval notification to VA will be accomplished: Security patches are applied by emergency updates via vendor only and a regular schedule through vendor services	

Can the device support the use of McAfee Anti-Virus (AV) software?	☐ Yes ☑ No
If no, what AV packages and versions are supported and describe the mechanism to provide updates.	
Can USB ports be disabled on the device without compromising operation?	☐ Yes ☑ No
Can auto run be disabled for portable media?	☐ Yes ☐ No
Can VA install host-based security components such as a firewall, host intrusion prevention system (HIPS), anti-malware software, and/or any other security suite software required to operate on the VA production network?	☐ Yes ☑ No

If "No" is the response to any of the above questions regardiung updates and anti-virus software, please explain further for each item in the space below.

Authentication and User Account

Is an administrator or power user account required to operate the device?	☐ Yes ☑ No
Can the device be made to require individual user authentication?	☑ Yes ☐ No
Does the device support password aging and strong user password accounts?	☐ Yes ☑ No
Does the device support auto logoff or/and session lock?	☑ Yes ☐ No
Does the system support the use of Active Directory for user authentication?	☐ Yes ☑ No
If yes, specify configuration requirements, LDAP etc.:	
Does the system support the use of PIV/Smart Card only authentication?	☐ Yes ☑ No

Data Handling

Specify which Electronic Protected Health Information ePHI data elements are stored on the device (e.g., last name, SSN, DOB):	
How many records with sensitive information can be stored on the device?	0
How long will they be retained on the device?	Operation/Transaction
Is ePHI encrypted prior to transmission?	☐ Yes ☐ No
If yes, what is the encryption mechanism(s)?	
What is the media used for long term storage?	
How is data transmitted to the storage repository (e.g. LAN, DVD, USB, etc.)? LAN	
Is ePHI stored only on a drive partition or a separate drive to assist with end-of-life media sanitization?	☐ Yes ☑ No
Will the medical device require data backups?	☐ Yes ☑ No
If yes, specify how the system and data are backed up and what media is used: Describe backup process: (data centers are lights out so this needs to be known up front)	
*Where will backups be stored and secured?	
Does the device have the ability to assign unique ID numbers (accession numbers) instead of using patient identifying information (e.g., Social Security Number)?	☐ Yes ☑ No
If yes, how is it generated?	
Does the device utilize a laptop for system operation?	☐ Yes ☑ No
If so, can the laptop be encrypted without impacting clinical functionality?	☐ Yes ☐ No
If yes, what encryption software can be used?	

Networking

What are the LAN bandwidth requirements for full connectivity/performance? What are the WAN bandwidth requirements for full connectivity/performance?	
Provide a comprehensive list of all TCP and UDP ports that are required for operation: **Note: If more space is needed, please attach the comprehensive list of ports required for operation to this document. Attach a network diagram showing all communication requirements.**	
How many fixed IP addresses does the device require?	
Is the device compatible with IP V6?	☑ Yes ☐ No
Vendors' products should be designed such that only ports required for the intended operation of the device are active. Are unused ports closed or disabled?	☑ Yes ☐ No
Can this be accomplished without impacting system operation?	☑ Yes ☐ No
Vendors' products should be designed such that only services required for the intended operation of the device are active. Are unused services (e.g., Telnet, IIS, etc.) disabled?	☐ Yes ☐ No
Can this be accomplished without impacting system operation?	☐ Yes ☐ No
Provide a comprehensive list of all services that are required for system operation:	
Can the device be serviced remotely?	☑ Yes ☐ No
Does the vendor have an existing Site to Site (S2S) VPN tunnel or individual user VPN account(s)?	☐ Yes ☐ No
What remote access software does the system utilize (e.g., Dameware, PC Anywhere, etc.)?	
Does the device require connection to the Internet to operate?	☑ Yes ☐ No
If yes, please justify and provide connection info (IP, port, protocol and traffic direction):	

Wireless

Does the device utilize wireless communication?	☐ Yes ☐ No
• If yes, what protocols are used?	
The encryption module must have FIPS 140-2 certification. Provide certificate number:	
Are any ePHI data elements transmitted via the wireless link?	☐ Yes ☐ No
• If yes, list each element (e.g. last name, DOB, SSN).	

Integration with VA Healthcare Information Systems (if applicable)

*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 bi-directional HL7 interface?	☐ Yes ☐ No
List all other systems that the device will communicate with in order to operate properly, e.g. VistA, domain controllers, vendor's support network, etc.:	

Signature Page

***Equipment Category (VA-MDNS):**	**Vendor:**
***Requesting Service:**	***Model:**

_____

Chief, Biomedical Engineering Date
Concur/Non-Concur

_____

Chief Information Officer Date
Concur/Non-Concur

_____

Information Security Officer Date
Concur/Non-Concur

Pre-Procurement Procedures and Exclusions

The following guidance updates previous VA Directive 6550 procedures and revises existing procedures/policies related to VA Handbooks 6500.6, and associated procurement guidance.

(1) Medical equipment procurement requests are forwarded to the facility or VISN Biomedical Engineer, depending on the scope of the procurement.

(2) Biomedical Engineering determines if the procurement requires completion of VA Directive 6550 Appendix A Form "VA Medical Device Pre-Procurement Assessment". If the device/system will be connected to the network and/or stores sensitive information, then this Form is required.

(3) Biomedical Engineering consults with OIT and the ISO during the pre-procurement planning process to ensure OIT and security needs are identified and input is provided.

(4) Biomedical Engineering completes the PPA, in collaboration with OIT.

(5) Biomedical Engineering forwards the completed PPA to the facility Chief Information Officer (CIO) or VISN CIO, depending on the scope of the procurement. The CIO will utilize the internal OIT Regional process to complete the PPA review within ten (10) business days. If there are outstanding questions requiring follow-up, OIT will forward the items to Biomedical Engineering. Biomedical Engineering will resubmit to OIT once outstanding issues have been resolved and the ten (10) business day review time will resume based on the date clarifications were submitted. OIT will review updated information and provided it addressed the questions, will concur and forward the signed PPA to the facility ISO.

(6) The facility ISO will review the request and within ten (10) business days. If there are outstanding questions requiring follow-up, the ISO will forward the items to Biomedical Engineering. Biomedical Engineering will resubmit to the ISO once outstanding issues have been resolved and the ten (10) business day review time will resume based on the date clarifications were submitted. The ISO will review updated information and provided it addressed the questions, will concur and forward the signed PPA back to Biomedical Engineering.

(7) Ensuring that every effort is made by Biomedical Engineering, OIT, and the ISO to reach consensus on medical device PPA review. For any items where outstanding issues remain that cannot be resolved by the Biomedical Engineering and OIT, the Medical Center Director, as the designated Medical Device/System Owner will review the risk analysis and make a risk-based decision to authorize or reject the acquisition. The risk–based decision shall consider clinical benefit to patient care on balance with

projected technical and/or security risks. Documentation of the risk-based decision shall be signed by the Medical Center Director and kept on record with Biomedical Engineering. These instances are expected to be extremely rare as every effort should be made to resolve technical risk issues in context of clinical capabilities before escalating to the Medical Center Director.

(8) Biomedical Engineering ensures completion of VA Handbook 6500.6 Appendix A or its electronic equivalent for all medical equipment procurements, regardless of the PPA status.

(a) If the procurement is for a medical device that is not network connected or does not store sensitive information, then VA Handbook 6500.6/A does not require review by the ISO or Privacy Officer (PO). In these instances, the Biomedical Engineer will sign and forward VA Handbook 6500.6/A directly to Contracting as part of the procurement package.

(b) For network connected medical devices or medical devices that store sensitive patient information, the Biomedical Engineer will complete the VA Handbook 6500.6/A and will forward on to the ISO and PO for review.

(9) Medical devices must be networked in accordance with the current version of VA's Medical Device Isolation Architecture (MDIA) guidance. With very limited exceptions, network-connected medical devices shall be isolated on a MDIA VLAN. As a component of implementation planning activities, Biomedical Engineering will generate the request for the MDIA VLAN configuration change and send required information to OIT per the MDIA Change Management SOP. The request will contain the device communication profile (e.g., host and target IP addresses, ports, and protocols) with sufficient detail to allow for the construction/modification of the access control list (ACL) or firewall rule. The MDIA change management process should be viewed as a component of the implementation planning activities and should be initiated during that phase.

(10) For systems with enterprise-wide deployment, deployment and implementation guidelines will be jointly developed by Healthcare Technology Management, Field Security Service, and OIT.