Department of Veterans Affairs
Washington, DC 20420

VA Directive 6550
Transmittal Sheet
June 3, 2019

PRE-PROCUREMENT ASSESSMENT AND IMPLEMENTATION OF MEDICAL DEVICES/SYSTEMS

1. **REASON FOR ISSUE:** This Directive establishes the technical Pre-Procurement Assessment (PPA) and Implementation requirements for medical devices/systems. This Directive covers medical devices/systems that are connected to the VA network and medical devices and systems that store sensitive patient information.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** Major changes include updating mandatory policy, responsibilities, definitions and inclusion of risk analysis and implementation processes.

3. **RESPONSIBLE OFFICE:** Veterans Health Administration (VHA) Office of Healthcare Technology Management (10NA9).

4. **RELATED DIRECTIVE/HANDBOOK:** VA Directive 6500, VA Handbook 6500.

5. **RESCISSION:** VA Directive 6550, February 20, 2015.

CERTIFIED BY:

/s/
Melissa S. Glynn, Ph.D.
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Richard A. Stone, M.D.
Executive in Charge, Veterans Health
Administration

DISTRIBUTION: Electronic only

PRE-PROCUREMENT ASSESSMENT AND IMPLEMENTATION FOR MEDICAL DEVICES/SYSTEMS

1. **PURPOSE.** This Directive establishes the technical Pre-Procurement Assessment (PPA) and Implementation requirements for medical devices and medical systems that are connected to the VA network or stand-alone medical devices that store sensitive patient information.

2. **BACKGROUND**.

   a. All medical devices/systems are assessed for a variety of factors during the acquisition process. These factors include but are not limited to clinical features/functionality, human factors engineering, safety, security, serviceability, reliability, integration requirements, and space and infrastructure utility requirements, such as power, air conditioning, and network connectivity.

   b. VHA Office of Healthcare Technology Management (HTM) is the owner for medical devices/systems, and Biomedical Engineering (BME) is responsible for lifecycle management of medical devices/systems within VA, facilitating input in defining requirements from clinical staff, and providing technical oversight of the medical device/system selection process. BME is also responsible for ensuring medical device/system purchases are reviewed by the appropriate stakeholders. BME staff located at medical facilities and Veterans Integrated Service Networks (VISNs) coordinate with Office of Information and Technology (OIT) staff to ensure that detailed technical assessments and security reviews are conducted prior to contracting and acquisition of medical devices/systems. OIT is the VHA IT service provider and is responsible for identifying and involving appropriate stakeholders to facilitate system implementation. OIT involvement at the local or national level is postured to provide customer support and guidance to ensure medical devices/systems under review can be safely and securely deployed on the VA network.

   c. Advances in medical technology and designs have impacted patient care, as medical devices/systems have an expanding capability to store patient data and connect to healthcare networks. There are many benefits to having network-connected medical devices/systems that store data, including the availability of patient data and diagnostic images for clinical staff, which facilitates more timely and effective care. However, use of network-connected medical technology poses potential risks for the healthcare facility, such as increased bandwidth competition on the VA network, increased risk for medical device/system exposure to malware, system integration challenges, increased data storage requirements, and increased chance of loss of sensitive patient data stored on medical devices/systems.

d. Evaluating the configuration and security profile of medical devices/systems during the acquisition and implementation planning processes will assist in identifying potential risks and provide for a more effective and safe integration of medical devices/systems into healthcare operations. Key stakeholders involved in this process are VHA Biomedical Engineering, OIT, and Information Assurance/Cybersecurity Analysts. Risk assessments for non-medical devices/systems adhere to a different process and are not covered in this Directive.

e. This VA policy defines a medical device/system as a non-IT device or system that meets one or more of the following requirements:

(1) Is 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 systems, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS), and laboratory analyzers. This includes medical devices/systems that directly connect to a patient, process human and other biologic specimens, create medical images, display electrophysiological waveforms, obtain physiologic measurements, and/or directly perform therapeutic-support to the patient.

(2) Has gone through the Food and Drug Administration's (FDA) Premarket Review or 510(k) 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.

f. VHA Office of Healthcare Technology Management (HTM) is responsible for determining whether equipment is classified as medical devices/systems. Medical devices/systems will be designated with a standard VA Medical Device Nomenclature System (VA MDNS) category, which VHA HTM maintains. VA MDNS is the authoritative source for medical device classification and can be used to determine equipment categories and define medical devices/systems within the VA inventory system(s). VA MDNS also identifies which equipment categories need to be placed behind the Medical Device Isolation Architecture (MDIA).

3. POLICY.

a. VHA has assigned responsibility for lifecycle management of medical devices and medical systems to VHA HTM and field-based Biomedical Engineering programs. To manage risks and ensure a safe healthcare environment, Biomedical Engineering leads the technical requirements definition and related PPA and implementation processes for all medical devices/systems as an integral aspect of medical technology lifecycle management.

b. The PPA serves as the multi-disciplinary (BME and OIT) technical review and approval process for network connected medical device/system procurements. As such, no additional OIT specific processes used solely for the procurement of IT assets are required or applicable. Additionally, if internal VA IT software development is not required to deploy the device/system and IT infrastructure is sufficient for the deployment, no additional VHA resource/project requests are required. Note that OIT Area Managers may be required to submit documentation via varying OIT processes for internal OIT purposes, but these processes are external to VHA and are outside the scope of this Directive.

c. PPAs shall be performed on all medical devices/systems that have the potential to be connected to the VA network or medical devices that store sensitive patient information. This helps to ensure that medical devices/systems are safely and securely integrated with VA's clinical and IT systems and networks. Biomedical Engineering leads the PPA process to ensure that appropriate assessment/review is performed by OIT prior to purchase. Biomedical Engineering shall confer with medical staff and equipment users regarding clinical requirements. VISNs and facilities will utilize Appendix A to initiate the PPA process for all applicable mdical devices/systems. The overall process is outlined in Appendix B, and the process flowsheet in Appendix C provides a high-level overview of the workflow.

d. The full PPA process for a new medical device/system consists of preparation of the following documents and transmission of these documents to the Specialized Device Security Division (SDSD). Submission of these documents to SDSD concludes the 6550-related pre-procurement assessment activities.

    (1) *6550 Appendix A* – the manufacturer completes the 6550 Appendix A, but BME is responsible for validating and finalizing the document with site-specific information and forwarding the document for signature and approval

    (2) *Manufacturer Disclosure Statement for Medical Device Security (MDS^2)* – vendors complete the MDS^2 and submit to BME

    (3) *Complete Ports, Protocols, and Services (PPS) list* – BME prepare the ports and protocols list using information within the 6550 Appendix A and MDS^2

    (4) *Topology diagram* – either BME or vendors prepare the topology diagram showing data flow and assessment boundary

    (5) *Complete hardware/software inventory* – BME provides a full system hardware/software inventory with a description of component purpose

e. Once the PPA documents are submitted to SDSD, the Enterprise Risk Analysis (ERA) process begins, and the procurement transitions to the initial stages of pre-implementation. SDSD reviews the submitted documents and follows up with BME and/or the medical device/system manufacturer to resolve outstanding questions. Once the ERA is completed, it will be signed by the Specialized Medical Device

Security Control Assessor (SCA) who completed the assessment and then forwarded for approval by the Medical Device Authorizing Official (AO).

f. New items will be continuously added to the ERA inventory as additional evaluations are completed and new medical devices/systems are released. If an existing ERA is in place for a functionally-similar item, BME will complete only Section 1 of the 6550 Appendix A, and that will conclude the 6550-related pre-procurement process. The existing ERA will be referenced for pre-implementation/deployment activities. If one or more of the characteristics change (e.g. new operating system, major software version change, etc.), then the full PPA process as described in paragraph 3(d) will be followed.

g. Facilities or VISNs can execute procurements for medical devices/systems while the ERA is being developed by the Medical Device SCA; however, deployment cannot proceed until the ERA is completed.

h. Server-based medical systems require a separate PPA for the server and client devices. For bulk procurements of identical medical equipment items, only one PPA is needed.

i. Implementation will be facilitated by this process as much of the network and security documentation will be developed via the ERA process. Biomedical Engineering is responsible to lead, or co-lead with clinical departments, the implementation planning for medical devices/systems. Biomedical Engineering shall identify interconnectivity requirements of the medical device and provide OIT staff with network communication and configuration information required to connect the device to a MDIA Virtual Local Area Network (VLAN). If a new VLAN is needed, Biomedical Engineering will enter an OIT request to create the MDIA VLAN and provide a link to the applicable ERA.

4. RESPONSIBILITIES.

a. **Network Directors.** Network Directors shall:

(1) Ensure facilities in their Network establish and execute Standard Operating Procedures that are consistent with the requirements of this Directive.

(2) Ensure consolidated medical equipment acquisitions and VISN-level medical system acquisitions meet the requirements outlined in this Directive.

(3) Ensure equipment planning and procurement 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 shall:

(1) Develop local facility Standard Operating Procedures that are consistent with requirements outlined in this Directive.

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

c. **Biomedical Engineering.** Biomedical Engineering staff shall:

(1) Ensure a quality assurance and lifecycle 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), The Joint Commission, VA policy and procedures, technical infrastructure, and cybersecurity risk management.

(2) Engage with clinical staff, local ISSOs, OIT staff, and contracting personnel in the development of applicable requests for proposals (RFPs)/requests for quotes (RFQs), and pre-procurement planning to ensure incorporation of applicable technical and architectural standards, IT capacity, and information security considerations.

(3) Ensure maintenance requirements for hardware and software are accounted for in pre-purchase planning. Coordination with OIT staff is needed for hardware, such as a virtual server, storage, or disaster recovery resources when OIT provides resources for the specific device or system.

(4) Coordinate with contracting to ensure vendors provide required documentation for procurement, implementation, integration, configuration, and sustainment of medical equipment.

(5) Complete the pre-procurement process in collaboration with manufacturer/vendor(s). Vendors should submit their MDS^2 form in the currently published version electronically to Biomedical Engineering in an Excel file.

(6) Forward the pre-procurement documents (6550 Appendix A and MDS^2) to the ISSO for procurements without an existing ERA.

(7) Forward 6550 Appendix A to the ISSO for procurements where there is an existing ERA in place.

(8) Provide the SCA with the PPA documentation (6550 Appendix A; MDS^2; complete ports, protocols, and services (PPS) list; topology diagram(s) showing data flow and assessment boundary; and complete inventory of system component hardware/software with a description of component purpose) to assist SCAs in completing an ERA for the device/system.

(9) Complete VA Handbook 6500.6 Appendix A for acquisition of medical equipment.

(10) Maintain completed copies of 6550 Appendix A, the MDS[2], communication profiles, and other relevant documents on file throughout the life of the medical device/system.

(11) Ensure procured medical devices/systems are aligned with applicable VHA national standards and guidelines.

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

(13) Identify interconnectivity requirements for the medical device and provide OIT staff with network communication and configuration information required to connect the device to a VLAN, e.g. communication profile and/or ACL change request, etc.

(14) Update the VHA Networked Medical Device Database (NMDD) during deployment, modification, or decommissioning of the medical device/system.

d. **Information Systems Security Officers (VISN ISSOs for VISN-wide procurements.)** ISSOs shall:

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

(2) Provide consultation on pertinent security precautions/requirements to protect the device and the network from malware.

(3) When required, assist in establishing a remote access process for the servicing vendor, via proper VA account establishment procedures.

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

(5) Determine whether the equipment manufacturer has an existing Business Associate Agreement (BAA) with VHA and initiate a new BAA request when required.

(6) Determine whether the equipment manufacturer has an existing Memorandum of Understanding/Interconnection Security Agreement (MOU/ISA) with VHA and initiate a new MOU/ISA request when required.

(7) Validate the OIS ERA repository to determine if a recent ERA has been completed. If so, provide Biomedical Engineering with a link to the document.

e. **OIS Specialized Device Security Division (SDSD).** SDSD shall:

(1) Serve as the Medical Device Security Controls Assessor (SCA) by reviewing documents, completing the ERA tool, and identifying mitigating controls, taking into consideration patient safety, technical requirements, and security risks.

(2) Serve as the Medical Device Authorizing Official (AO) Designated Representative by signing the completed ERA package for the authorization to connect.

f. **Facility OIT Area Managers (Directors of IT Operations for VISN-wide procurements).** Facility OIT Area Managers shall:

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

(2) Actively participate in local and VISN Equipment Committees to provide input/assessment of IT infrastructure capacity and requirements.

(3) Engage OIT members at the appropriate level to coordinate resources when significant OIT infrastructure resources will be required to support requested medical devices/systems. OIT Area Managers will be responsible for preparation and submittal of the IT resource requests (virtual server, disaster recovery, Wide Area Network (WAN), etc.) for their VHA customers.

(4) Review and concur with the acquisition of network connected client/server based medical systems from an IT capacity, operations, integration and technical perspective to ensure that OIT support roles and responsibilities are identified.

(5) Provide virtual and physical access to Biomedical Engineering for the deployment and ongoing support of medical devices/systems.

g. **Deputy Under Secretary of Health for Operations Management (DUSHOM).** The DUSHOM shall: Serve as the designated medical device system owner.

h. **Contracting Officers.** Contracting Officers shall:

(1) Require all offerors to submit 6550 Appendix A and MDS^2 forms as part of their RFP/RFQ response for applicable equipment.

(2) Ensure that medical device security is an evaluation criterion in RFP/RFQ documents for applicable equipment.

5. REFERENCES.

a. Healthcare Information and Management Systems Society (HIMSS) and the National Electrical Manufacturers Association (NEMA), *Manufacturer Disclosure Statement for Medical Device Security (MDS2).*

b. VA Directive 6500, *VA Cybersecurity Program,* January 24, 2019.

c. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3 VA Information Security Program,* March 10, 2015.

d. VA Handbook 6500.6, *Contract Security,* March 12, 2010.

e. VHA Handbook 1605.05, *Business Associate Agreements,* July 22, 2014.

f. National Institute for Standards and Technology (NIST).

g. Federal Information Security Management Act of 2002 (FISMA).

h. Food and Drug Administration (FDA).

i. The Joint Commission (TJC).

j. VA Enterprise Risk Analysis (ERA) website.

VA DIRECTIVE 6550 Appendix A – To be completed for all procurements of network-connected medical devices and non-network-connected medical devices that store sensitive information. For client/server systems, a separate 6550 Appendix A is required for each the client and the medical server.

1.1	Equipment Category (VA-MDNS)	
1.2	Manufacturer	
1.3	Model	
1.4	NSI Number (if known)	
1.5	Application Name and Software Version #	
1.6	Requesting Service	
1.7	VISN	
1.8	Facility Name	
1.9	Facility Number	
1.10	Manufacturer Point of Contact	
	Phone Number	
	E-mail address	
1.11	Biomedical Engineering Point of Contact	
	Phone Number	
	E-mail address	
1.12	Responsible Service if Biomedical Engineering is NOT the Primary System Manager for system maintenance, support and lifecycle management	
1.13	Medical Device Type	□ Discrete device □ Software □ Client □ Application server
1.14	Device Description (i.e. equipment function and systems it communicates with)	
1.15	MDIA VLAN Number for installation (if known)	
1.16	Device Operating System (OS) *Please include OS build level.* *Review support status for* ***Windows OS*** *versions* *here*.	
Procurement of devices with unsupported operating systems is prohibited. Unsupported operating systems are OSs that are not supported by the manufacturer and have reached the end of the OS lifecycle as published by the OS manufacturer (i.e. no further security patches will be released for the OS by the manufacturer after the OS end-of-life nor will be available by other methods such as extended warranty purchases from the OS manufacturer).		
1.17	Does the device support wireless network connection?	□ Yes □ No
	If yes, what is the FIPS 140-2 or 140-3 certification number?	
	If no, does the vendor support the installation of FIPS 140-2 or 140-3 wireless cards?	□ Yes □ No
Procurement of devices using 802.11 wireless networking that are not FIPS 140-2 or 140-3 compliant is prohibited.		
1.18	Does the device have an existing, active Enterprise Risk Analysis (ERA)?	□ Yes □ No
	If yes, what is the ERA number?	
	If the device has a direct connection to Cerner or **EHRM interface**, does the device have an existing **MedMod ERA**?	□ Yes □ No
	If yes, what is the **MedMod ERA** number?	
	***Note that the ERA must be for the same make, model, and application software version to apply to the requested device. A new ERA is required for major software or operating system updates (e.g. version 2.0 to 3.0) but is not required for minor updates (e.g. version 2.0 to version 2.1).*	
If an ERA exists for the requested device, completion of the 6550 Appendix A is not required beyond this point. Please sign to certify that an existing ERA is available for the requested device and forward the document to either the Area Manager or ISSO for signature, as appropriate. Please note that if the device is an EHRM device, a MedMod ERA is required.		

2.1	Can the OS be automatically patched?	☐ Yes ☐ No
	***Note that devices that do not support automated patching via the VHA MD Update Server (MDUS) or via vendor channels impose a significantly higher risk to the VA network.*	
	If patching is not automated, what is the patching process and/or limitations?	
2.2	For applications and sub-applications (e.g., Java, Apache) on the device, is automatic patching or updating supported?	☐ Yes ☐ No
	***Note that devices that do not support automated patching impose a significantly higher risk to the VA network.*	
	If patching is not automated, what is the patching process and/or limitations?	
2.3	Is a device hardening guide available?	☐ Yes ☐ No
2.4	Does the device have logging or other auditing mechanisms in place?	☐ Yes ☐ No
	If yes, can these logs be exported to a syslog or similar server?	
2.5	Does the device include a database?	☐ Yes ☐ No
	If yes, what is the database version and type (e.g., SQL, Oracle)?	
	***Note that procuring and deploying devices with unsupported database versions imposes a significantly higher risk to the VA network.*	
	Does the vendor support database conversion from SSN to electronic data interchange personal identifier (EDIPI)?	☐ Yes ☐ No ☐ No PHI
	Does the vendor database support multiple identifiers?	☐ Yes ☐ No ☐ No PHI
2.6	Can the device run Defender, ESET, or McAfee antivirus?	☐ Yes ☐ No
	***Note that devices that do not support VA-approved antivirus scanning or an antivirus scanning solution managed by the vendor impose a significantly higher risk to the VA network.*	
	If antivirus is not supported, what are the AV processes and/or the limitations?	
2.7	Can a commercial-off-the-shelf (COTS) endpoint management system be installed (e.g., IBM Big Fix, Goverlan, SCCM)?	☐ Yes ☐ No
	If so, which one(s)?	
2.8	For Windows-based devices, can the existing Microsoft service be enabled to communicate with the VHA SMAK-AM server?	☐ Yes ☐ No ☐ Non-Windows-based system
	If no, has the vendor agreed to provide a complete software and application inventory for all system components as per FISMA requirements?	☐ Yes ☐ No
	***Note that devices that do not support communication with the SMAK-AM server or for which the vendor does not agree to provide a complete software inventory impose a significantly higher risk to the VA network.*	
2.9	Does the device support the use of two-factor authentication?	☐ Yes ☐ No
	***Note that devices that do not support two-factor authentication impose a significantly higher risk to the VA network. Please review the VA's requirements for two-factor authentication here.*	
	Does the device require interactive login service accounts?	
	***Note that devices that require interactive login service accounts impose a significantly higher risk to the VA network.*	
2.10	Will the device be joined to the VA domain?	☐ Yes ☐ No
	***Note that devices that are not joined to the domain impose a significantly higher risk to the VA network.*	
2.11	Does the device allow for encryption of the data drive or OS drives?	☐ Yes ☐ No
	What level of encryption is allowed?	
2.12	Are post-quantum cryptography (PQC) ciphers being used for this implementation?	☐ Yes ☐ No

2.13	What method of encryption is used for data in transit?	☐ SSL ☐ HTTPS ☐ TLS (version: ______________________) ☐ SFTP ☐ None ☐ Other:	
	***Note that use of SSL is prohibited and that TLS versions 1.0/1.1 impose a significantly higher risk to the VA network.*		
2.14	Is sensitive data stored at rest on the device?	☐ Yes ☐ No	
	If yes, how many records can be stored on the device?	☐ <500 ☐ >500	
	If yes, does the device support on demand purging of data from the local hard drive?	☐ Yes ☐ No	
2.15	Will sensitive data be stored outside of the VA network (e.g. cloud-based service provider – excludes Electronic Medical Record connection)?	☐ Yes ☐ No	
2.16	Does the device send/receive VA data to/from an external, vendor-managed cloud?	☐ Yes ☐ No	
	If yes, has the cloud platform been approved by the VA Digital Transformation Center (DTC)? *To determine approval status, please visit the Digital VA Product Marketplace.*	☐ Yes ☐ No	
	If yes, what is the cloud type, determined by the VA DTC?	☐ Software as a Service (SaaS) ☐ Managed Service	
	If SaaS, what is the FedRAMP package ID?		
	If SaaS, is it FedRAMP authorized?	☐ Yes ☐ No	
	Is there an approved VA ATO for the cloud platform?	☐ Yes ☐ No	
2.17	Is connectivity external to the VA required for device operation?	☐ Yes ☐ No	
2.18	Is connectivity external to the VA required for device support?	☐ No ☐ Yes - VA S2S VPN ☐ Yes - VA Citrix ☐ Yes – VA Azure Virtual Desktop ☐ Yes – Other	
	If other, describe the remote access method.		
	What is the MOU/ISA number?		
2.19	How many IP addresses are required?		
2.20	What kind of IPs does the device use?	☐ Static IP ☐ DHCP	
	***Devices should be deployed with static IPs unless DHCP is required.*		
2.21	Is IPv6 supported?	☐ Yes ☐ No	
	If yes, please list any limitations.		
2.22	If server-based, select one from each column:	☐ Vendor-provided ☐ VHA-provided ☐ Other - describe	☐ Physical server ☐ Virtual host ☐ Cloud virtual host
2.23	If server-based, list server specifications (cores, RAM, power, storage) and rack space. *Attach additional documentation, as needed.*		
2.24	Does the device use Java?	☐ Yes ☐ No	
2.25	Does the device utilize machine learning/artificial intelligence?	☐ Yes ☐ No	
2.26	What type of vulnerability scanning is allowed on the device?	☐ Active ☐ Passive ☐ Both	
	If active, is credentialed scanning allowed?	☐ Yes ☐ No	

2.27	If the device uses digital signatures, is it compliant with FIPS 186-4?	☐ Yes ☐ No ☐ N/A
2.28	Does this system include a pre-production (test) environment?	☐ Yes ☐ No
2.29	Does the device support backups?	☐ Yes ☐ No
	Does this procurement include a backup solution?	☐ Yes ☐ No ☐ N/A
2.30	Does this device include an HL7 interface?	☐ Yes ☐ No
	If yes, what will the HL7 interface be used for?	☐ Orders ☐ Results ☐ Billing (DFT) ☐ ADT ☐ Other: ________________________
If the requested device does not have an EHRM approved connection or interface to Cerner, completion of the 6550 Appendix A is not required beyond this point. Please sign this document and route it for signature, as appropriate.		
2.31	Does the device have an EHRM approved Cerner interface? *For more information, please reference the approved EHRM interface list and the EHRM IO HTM SharePoint site*	☐ Yes ☐ No
	If no, has an NSR been submitted for interface approval?	☐ Yes ☐ No NSR Number:
	If no, to which security authorization boundary will this device/system be added? *For more information on MedMod zones and MD-LITE, please reference the EHRM IO HTM SharePoint site or contact the EHRM IO HTM team at EHRMIOHTM@va.gov.*	☐ MedMod Zone 6A ☐ MedMod Zone 6B ☐ MD-LITE ☐ Other ________________________________
	If no, what is the proposed EHR connection(s)/integration(s) type(s)? *For additional guidance, please contact the EHRM IO HTM team at EHRMIOHTM@va.gov.*	☐ Openlink (HL7) ☐ Compass Router (DICOM) ☐ EHR Gateway (Non-DICOM Image Routing) ☐ Cerner Connectivity Engine (CCE) ☐ CCE Terminal Server (CCE-TS) ☐ Separate HL7 Interface/Middleware Server ☐ None ☐ Other: ________________________

Submittal/Approval

____

Biomedical Engineering *Date*

____

*Area Manager** *Date*

**Area manager signature only required for client/server medical systems. Please sign within 10 business days of receipt.*

____

*Information Systems Security Officer*** *Date*

*** Please sign within 5 business days of receipt and return the document to Biomedical Engineering and the Area Manager. If an ERA is required, please submit this form with the ERA package to the Specialized Device Cybersecurity Department (SDSD) to initiate the ERA process.*

APPENDIX B – PRE-PROCUREMENT AND IMPLEMENTATION WORKFLOW

The following guidance updates previous VA Directive 6550 procedures and associated procurement guidance.

Pre-Procurement

(1) The using service submits a medical equipment procurement request. Requests are forwarded to either the facility or VISN Biomedical Engineering Manager for review, depending on the scope of the procurement.

(2) Biomedical Engineering determines if the medical device/system being requested is capable of being deployed with a network connection and/or storing sensitive information. If either of those conditions is met, Biomedical Engineering initiates the 6550 process as outlined below. For equipment that does not meet either of those conditions, Biomedical Engineering signs and submits VA Handbook 6500.6 Appendix A per local procurement procedures. The 6550 process is required for all medical devices/systems capable of being deployed with a network connection and/or storing sensitive information, regardless of whether the VA intends to connect the medical device/system to the network or store sensitive information.

(3) For equipment meeting the above criteria, Biomedical Engineering can assist the Contracting Officer in making the determination relative to the appropriate contract type (limited/sole source or a full and open competitive Request for Proposal (RFP)/Request for Quote (RFQ)). Biomedical Engineering will also determine if an Enterprise Risk Analysis (ERA) is in place for the requested procurement. Note - A new ERA is required for major software or operating system updates (e.g. version 2.0 to version 3.0) but is not required for minor updates (e.g. version 2.0 to version 2.1).

************************PROCUREMENT SCENARIOS************************

A. For Limited/Sole Source medical equipment procurements without an existing ERA in place, follow the steps below:

i. Biomedical Engineering obtains a completed electronic Manufacturer Disclosure Statement for Medical Device Security (MDS^2) form from the manufacturer.

ii. Biomedical Engineering completes 6550 Appendix A based on information provided in the MDS^2 and via consultation with the manufacturer. Note that Appendix A can be forwarded to the manufacturer for completion of the device specific information, but Biomedical Engineering is responsible for completing the site-specific data and validating the information using the MDS^2 and other technical information available from the manufacturer.

iii. Biomedical Engineering forwards the 6550 Appendix A and MDS^2 to the ISSO as part of the procurement of discrete devices. If the procurement is for a client/server system, Biomedical Engineering first sends Appendix A and the MDS^2 to the OIT Area Manager for signature. The Area Manager signature on Appendix A is required within 10 business days of receipt, and ISSO signature is required within 5 business days of receipt.

iv. The ISSO returns the signed 6550 Appendix A to Biomedical Engineering and forwards a copy of the signed 6550 Appendix A to the Area Manager. Biomedical Engineering forwards the 6550 Appendix A; MDS^2; complete ports, protocols, and services (PPS) list; topology diagram(s) showing data flow and assessment boundary; and a complete inventory of system component hardware/software with a description of component purpose to the OIT Specialized Devices Security Division (SDSD) to initiate the ERA process.

v. Once Appendix A is signed by the ISSO, the procurement package is sent to Contracting according to local procedures, and procurement action proceeds while the ERA is being completed by the Medical Device Security Controls Assessor (SCA).

(4) For new ERAs, the Medical Device Authorizing Official (AO) will review the ERA and will authorize or reject deployment based on the mitigating controls being proposed. The review shall consider clinical benefit to patient care on balance with projected technical and/or security risks. Documentation of the review and its outcome shall be signed by the Medical Device AO.

(5) After the ERA is signed, The Medical Device SCA notifies the identified BME point of contact (POC) that the ERA package has been completed.

B. For Limited/Sole Source procurements for medical equipment with an ERA already in place, follow the steps below:

i. Biomedical Engineering completes the top portion of 6550 Appendix A and forwards it to the ISSO for signature. If the procurement is for a client/server system, Biomedical Engineering first sends the 6550 Appendix A to the OIT Area Manager for signature. The Area Manager signature is required within 10 business days of receipt, and ISSO signature is required within 5 business days of receipt.

ii. The ISSO signs the 6550 Appendix A and provides a copy to Biomedical Engineering and the OIT Area Manager.

iii. Procurement package is sent to Contracting according to local procedures.

C. For competitive procurements for which the medical equipment manufacturer is not known, follow the steps below:

i. Contracting requires all bidders to submit 6550 Appendix A and MDS^2 forms as part of their proposal response.

ii. The technical evaluation team incorporates the security posture of the device/system in its evaluation and makes a selection based on the criteria outlined in the RFP/RFQ. Referencing the MDS^2, Biomedical Engineering completes the 6550 Appendix A for the preferred equipment vendor and forwards 6550 Appendix A and the MDS^2 form to the ISSO via the steps above (new or existing ERA).

iii. If Contracting awards to a vendor other than the vendor selected by the technical evaluation team, then Biomedical Engineering will complete a new 6550 Appendix A for the awarded equipment/vendor and will resubmit 6550 Appendix A and the MDS^2 form to the ISSO.

Implementation

As part of the post-procurement deployment/implementation process, Biomedical Engineering and OIT isolate the device in accordance with the current version of VA's Medical Device Isolation Architecture (MDIA) guidance. With very limited exceptions, all network-connected medical devices shall be isolated on a MDIA VLAN. Biomedical Engineering generates the request for the MDIA VLAN configuration change and sends required information to OIT.

(1) Biomedical Engineering determines if a new VLAN is needed or if an existing VLAN can be used to isolate the medical device on the network.

a. If a new VLAN is needed, Biomedical Engineering enters an OIT request for MD VLAN creation and provides the risk analysis report (RAR) with the request.

(2) Biomedical Engineering provisions IP addresses from a new or existing MD VLAN and creates a NMDD placeholder to prevent duplication.

(3) Biomedical Engineering develops or modifies the ACL using the ACL Comm Profile Template, the vendor’s list of ports and protocols, and the MDIA ACL Guide then submits an OIT request for the ACL creation/change.

(4) Biomedical Engineering enters an OIT request to ensure the new VLAN has been applied to the switch port where the device will be connected. Local OIT staff will identify the specific switch and port that is patched to the wall jack where the device will be installed.

(5) Biomedical Engineering names the systems using the approved naming conventions, ensuring all BME servers include Clinical Care Applications (CCA) and all BME workstations or devices include Medical Device (MD).

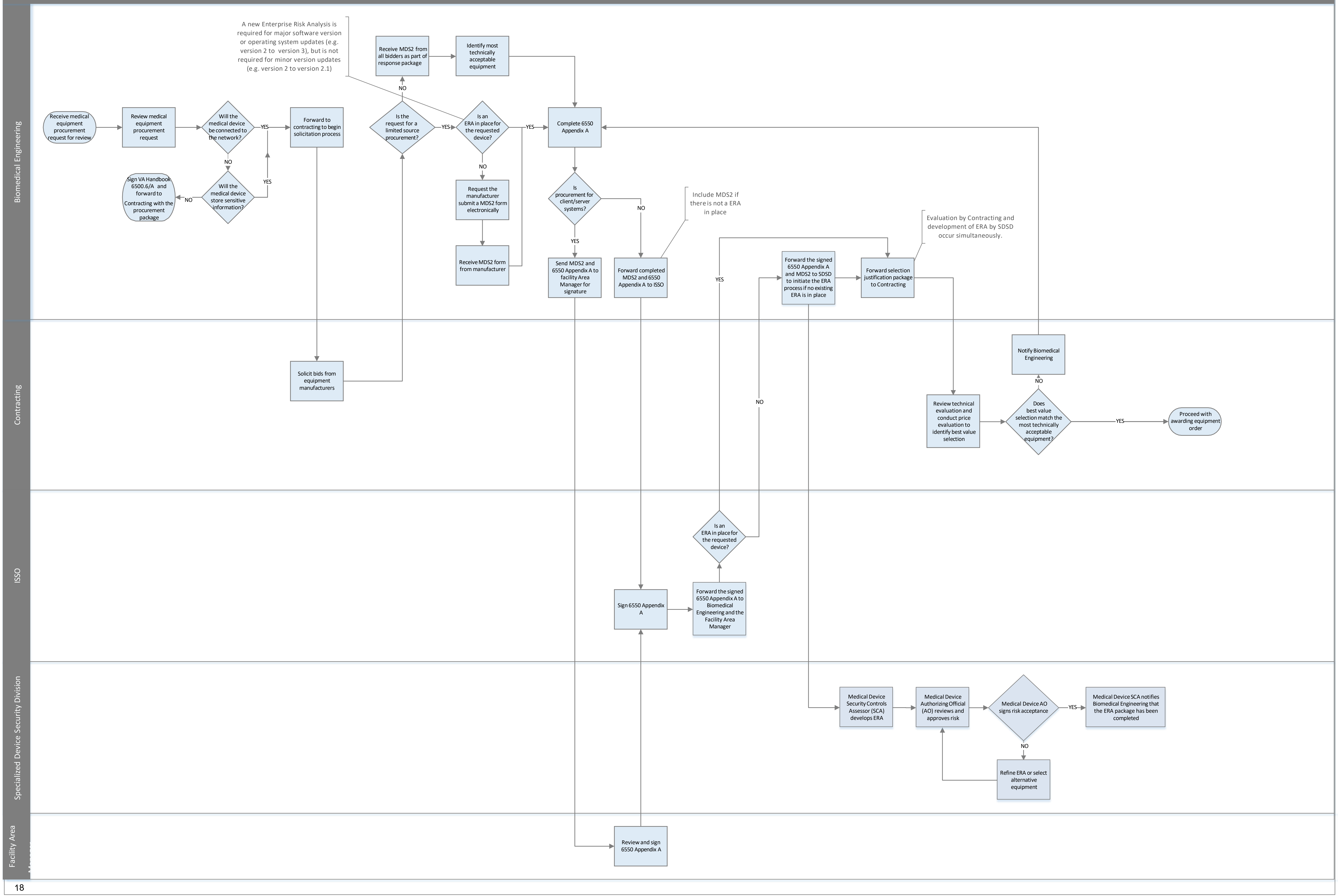
(6) For domain-connected systems, Biomedical Engineering enters an OIT request with the signed RAR to pre-stage the computer name within the Specialized System Organizational Unit (SSOU) for Medical Devices (refer to AD OU Configuration Guidance). This step is not required for non-domain-connected systems.

(7) For systems requiring remote vendor access, Biomedical Engineering works with the local ISSO to make the required changes in the site-to-site configuration or establish vendor accounts through Citrix.

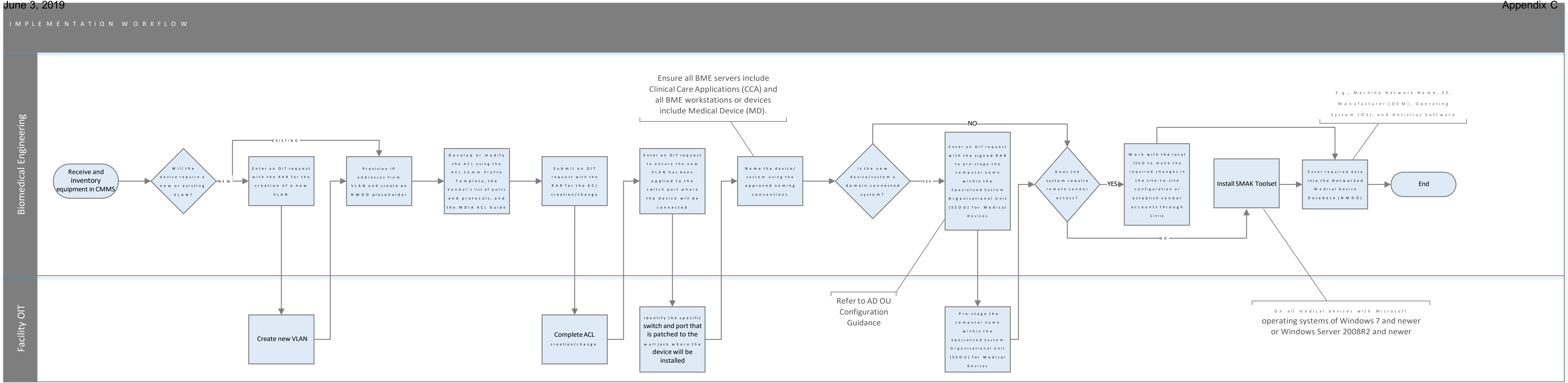
(8) For all medical devices with Microsoft operating systems of Windows 7 and newer or Windows Server 2008R2 and newer, with vendor approval, Biomedical Engineering installs the SMAK toolset on the medical device prior to deployment. If the vendor does not approve installation of the SMAK toolset, Biomedical Engineering requests a complete software and application inventory for all system components as per FISMA requirements.

(9) Biomedical Engineering enters required data into the Networked Medical Device Database (NMDD), including Machine Network Name, EE, Manufacturer (OEM), Operating System (OS), and Antivirus Software.

PRE-PROCUREMENT WORKFLOW


Biomedical Engineering
Contracting
ISSO
Specialized Device Security Division
Facility Area Manager
Receive medical equipment procurement request for review
Review medical equipment procurement request
Will the medical device be connected to the network?
YES
NO
Will the medical device store sensitive information?
YES
NO
Sign VA Handbook 6500.6/A and forward to Contracting with the procurement package
Forward to contracting to begin solicitation process
Solicit bids from equipment manufacturers
Is the request for a limited source procurement?
YES
NO
A new Enterprise Risk Analysis is required for major software version or operating system updates (e.g. version 2 to version 3), but is not required for minor version updates (e.g. version 2 to version 2.1)
Receive MDS2 from all bidders as part of response package
Identify most technically acceptable equipment
Is an ERA in place for the requested device?
YES
NO
Request the manufacturer submit a MDS2 form electronically
Receive MDS2 form from manufacturer
Complete 6550 Appendix A
Is procurement for client/server systems?
YES
NO
Send MDS2 and 6550 Appendix A to facility Area Manager for signature
Forward completed MDS2 and 6550 Appendix A to ISSO
Include MDS2 if there is not a ERA in place
Review and sign 6550 Appendix A
Sign 6550 Appendix A
Forward the signed 6550 Appendix A to Biomedical Engineering and the Facility Area Manager
Is an ERA in place for the requested device?
YES
NO
Forward the signed 6550 Appendix A and MDS2 to SDSD to initiate the ERA process if no existing ERA is in place
Forward selection justification package to Contracting
Evaluation by Contracting and development of ERA by SDSD occur simultaneously.
Review technical evaluation and conduct price evaluation to identify best value selection
Does best value selection match the most technically acceptable equipment?
YES
NO
Notify Biomedical Engineering
Proceed with awarding equipment order
Medical Device Security Controls Assessor (SCA) develops ERA
Medical Device Authorizing Official (AO) reviews and approves risk
Medical Device AO signs risk acceptance
YES
NO
Medical Device SCA notifies Biomedical Engineering that the ERA package has been completed
Refine ERA or select alternative equipment

IMPLEMENTATION WORKFLOW


Biomedical Engineering
Facility OIT
Receive and inventory equipment in CMMS
Will the device require a new or existing VLAN?
EXISTING
NEW
Enter an OIT request with the RAR for the creation of a new VLAN
Create new VLAN
Provision IP addresses from VLAN and create an NMDD placeholder
Develop or modify the ACL using the ACL Comm Profile Template, the Vendor's list of ports and protocols, and the MDIA ACL Guide
Submit an OIT request with the RAR for the ACL creation/change
Complete ACL creation/change
Enter an OIT request to ensure the new VLAN has been applied to the switch port where the device will be connected
Identify the specific switch and port that is patched to the wall jack where the device will be installed
Ensure all BME servers include Clinical Care Applications (CCA) and all BME workstations or devices include Medical Device (MD).
Name the device/system using the approved naming conventions
Is the new device/system a domain-connected system?
YES
NO
Enter an OIT request with the signed RAR to pre-stage the computer name within the Specialized System Organizational Unit (SSOU) for Medical Devices
Refer to AD OU Configuration Guidance
Pre-stage the computer name within the Specialized System Organizational Unit (SSOU) for Medical Devices
Does the system require remote vendor access?
YES
NO
Work with the local ISSO to make the required changes in the site-to-site configuration or establish vendor accounts through Citrix
Install SMAK Toolset
On all medical devices with Microsoft operating systems of Windows 7 and newer or Windows Server 2008R2 and newer
Enter required data into the Networked Medical Device Database (NMDD)
E.g., Machine Network Name, EE, Manufacturer (OEM), Operating System (OS), and Antivirus Software
End