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➔ / **STORAGE➓**	**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)