

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?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Does the device incorporate a switch or hub into its design?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Is the switch or hub required as part of the system configuration?	<input type="checkbox"/> YES	<input type="checkbox"/> 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?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• If server based, does the system utilize an ActiveX control for client interaction?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• If yes, specify configuration requirements.			
Authentication and User Accounts			
• Is an administrator or power user account required to operate the device?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Is an administrator account required for service?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Can the device be made to require user authentication?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Does user authentication support Strong Passwords?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Does user authentication support password aging?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Can the device be part of the facility's Windows domain?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
Data Handling			
• Will the medical device require data backups??	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Is ePHI stored only on a drive partition to assist with end of service media sanitization?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• What ePHI data elements are stored on the device?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Can ePHI be stored directly to a network drive, rather than local (machine) storage?	<input type="checkbox"/> YES	<input type="checkbox"/> 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?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Can the device support DHCP for network address configuration?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• How many IP addresses does the device require?			
• Can the device operate properly without connection to the Internet?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Can the target system be addressed via a fully qualified domain name (FQDN)?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
Wireless			
• Does the device utilize wireless communication?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• If so, what protocols are used?			
• Is any ePHI transmitted via the wireless link?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• Does the device support installation of FIPS 140-2 certified wireless security clients?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
• If so, which ones?			
Integration with VA Health Care Information Systems (if applicable)			
• Has the device been validated with VA's Clinical Procedures package?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
• Has the device been validated with VA's Vista Imaging?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
• Does the device have a bi-directional HL7 interface?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
• DICOM conformance statement provided.	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A

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:

IT POC:

Phone:

ISO:

Phone:

Medical Equipment Documentation Review

- ☐ Manufacturer Disclosure Statement for Medical Device Security (MDS²)
- ☐ 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 (security patches, software updates, maintenance support)
- ☐ Post implementation secure use strategy developed (i.e. frequency of removal of ePHI from device, physical security of device, etc.)

Manufacturer Disclosure Statement for Medical Device Security--MDS²

Device Category *		Manufacturer *		Document ID	Document Release Date
Device Model		Software Revision		Software Release Date	Other
Manufacturer or Representative Contact Information	Name		Title		Department
	Company Name		Telephone Number		E-mail

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (PHI) <i>As defined by HIPAA Security Rule, 45 CFR Part 164</i>	Yes	No	N/A	Note #
1. Can this device transmit or maintain <i>electronic Protected Health Information</i> (ePHI)?				
2. Types of ePHI data elements that can be maintained by the device:				
a. Demographic (e.g., name, address, location, unique identification number)?				
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?				
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiological data with identifying characteristics)?				
d. Open, unstructured text entered by device user/operator?				
3. Maintaining ePHI: <i>Can the device</i>				
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?				
b. Store ePHI persistently on local media?				
c. Import/export ePHI with other systems?				
4. Mechanisms used for the transmitting, importing/exporting of ePHI: <i>Can the device</i>				
a. Display ePHI (e.g., video display)?				
b. Generate hardcopy reports or images containing ePHI?				
c. Retrieve ePHI from or record EPHI to removable media (e.g., disk, DVD, CD_ROM, tape, CF/SD card, memory stick)?				
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?				
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?				
f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?				
g. Other _____				

ADMINISTRATIVE SAFEGUARDS	Yes	No	N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?				
6. What underlying operating system(s) (including version number) are used by the device? _____				

PHYSICAL SAFEGUARDS	Yes	No	N/A	Note #
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)?				
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?				
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?				

TECHNICAL SAFEGUARDS	Yes	No	N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device?				
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?				
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?				
b. Can the device log provide an audit trail of remote-service activity?				
c. Can security patches or other software be installed remotely?				
12. Level of owner/operator service access to device operating system: <i>Can the device owner/operator?</i>				
a. Apply device manufacturer-validated security patches?				
b. Install or update antivirus software?				
c. Update virus definitions on manufacturer-installed antivirus software?				
d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)?				
13. Does the device support user/operator specific ID and password?				
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?				
15. Events recorded in device audit log (e.g., user, date/time, action taken): <i>Can the audit log record</i>				
a. Login and logout by users/operators?				
b. Viewing of ePHI?				
c. Creation, modification or deletion of ePHI?				
d. Import/export or transmittal/receipt of ePHI?				
16. Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use?				

17.	Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?		
18.	Controls when exchanging ePHI with other devices:		
a.	Transmitted only via a physically secure connection (e.g., dedicated cable)?		
b.	Encrypted prior to transmission via a network or removable media?		
c.	Restricted to a fixed list of network addresses (i.e., host-based access control list)?		
19.	Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?		

Manufacturer Disclosure Statement for Medical Device Security--MDS²

RECOMMENDED SECURITY PRACTICES

EXPLANATORY NOTES (from questions 1 – 19)

IMPORTANT: Refer to Instructions for the Manufacturers Disclosure Statement for medical Device Security for the proper interpretation of information provided in this form.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.