Medical Equipment Pre-Procurement Assessment

Medical Equipment Evaluation Matrix

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, 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 medical equipment 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?	☐ YES	☐ NO	
• 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 – list all?	_____		
• 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 (if applicable)			
• Has the device been validated with VA's Clinical Procedures package?	☐ YES	☐ NO	☐ N/A
• Has the device been validated with VA's Vista Imaging?	☐ YES	☐ NO	☐ N/A
• Does the device have a bi-directional HL7 interface?	☐ YES	☐ NO	☐ N/A
• DICOM conformance statement provided.	☐ YES	☐ NO	☐ N/A

Manufacturer Disclosure Statement for Medical Device Security--MDS[2]

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) *As defined by HIPAA Security Rule, 45 CFR Part 164*	Yes No N/A	Note #
1.	Can this device transmit or maintain *electronic Protected Health Information* (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: *Can the device*		
	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: *Can the device*		
	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: *Can the device owner/operator?*		
	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): *Can the audit log record*		
	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--MDS[2]

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.