DEFENSE HEALTH AGENCY (DHA) Medical Cybersecurity

693 Neiman Street
Ft. Detrick, Maryland 21702

Medical Device and Equipment Risk Assessment

(MDERA)

Version 6.4.1

To ascertain security compliance that is in agreement with United States Federal Government (USFG), Department of Defense (DoD), and Defense Health Agency (DHA) policies and directives, the vendor is required to complete the following Medical Device Equipment Readiness Assessment Questionnaire (MDERA) as part of the Request for Offer (RFO)/Risk Management Framework (RMF) Change Control Board (CCB) review process.

All Medical Systems/Devices are required to meet DoD cybersecurity and National Institute of Standards and Technology (NIST) standards, regardless of network connection type. The information provided below will be used as a pre-procurement selection tool used to support all stakeholders working to achieve a Risk Management Framework (RMF) Authorization. Failure to disclose all required information, or misrepresentation of the proposed system's capabilities, will result in the system being ineligible for purchase, or result in a breach of contract and cancellation of contract if discovered after award.

The information provided below which includes data processing capabilities, current security posture, and level of compliance with the cybersecurity principles of Confidentiality, Integrity, and Availability will be used to identify the technical characteristics of the Medical System/Device and determine the level of effort and potential actions required prior to and during an RMF Assessment process, from a cybersecurity standpoint.

Revision History

Date	Section/Item	Comments	Author
22-Jan-19	Full Document	Initial draft.	Andrew McGraw
28-Mar-19	Full Document	Removal of technical requirements not required during the RFI phase.	Andrew McGraw
6-Jan-20	Full Document	Addition of Section 3: Data Processing Capabilities. Clarified and enhanced questions in Section 2.	Andrew McGraw
9-Dec-20	2.7	Added section to 2.7 describing methods for testing compliance of the device.	Andrew McGraw
17 Mar 21	Full Document	Removed references to CyberLOG.	Andrew McGraw
11-15-21	Full Document	Combining ICS and CyberLOG requirements	Andrew McGraw
10-17-22	Full Document	Requirement to identify country of origin for components and software.	Andrew McGraw
12-28-22	Full Document	Edits to fields, Version 6.3	Andrew McGraw
9-18-23	Full Document	Edits to fields, Version 6.4	Dr. Traci Moxley
2-20-24	Section 1.13; 2.11.1; 3.9; 3.10	Add USB Flash Drive	Dr. Traci Moxley

READ BEFORE PROCEEDING:

THIS SECTION OF THE MEDICAL DEVICE AND EQUIPMENT RISK ASSESSMENT (MDERA) QUESTIONNAIRE IS TO BE COMPLETED BY THE COMMERCIAL VENDOR IN ITS ENTIRETY AS PART OF THE MEDICAL DEVICE & EQUIPMENT (MDE) REQUEST FOR INFORMATION (RFI) PROCESS. THEREFORE, ALL INFORMATION FIELDS MUST BE ADDRESSED. REFERENCES TO EXTERNAL DOCUMENTS OR PRODUCT LITERATURE ARE NOT ACCEPTABLE.

ONCE COMPLETED, SUBMIT THE MDERA TO THE DESIGNATED POINT OF CONTACT (POC). IF THE POC IS UNKNOWN, SUBMIT THE COMPLETED MDERA TO THE CYBERLOG ORG BOX: DHA.DETRICK.MED-LOG.MBX.CYBERLOG@MAIL.MIL or ICS ORG BOX: DHA.DETRICK.PEO-MED-SYS-J-6.MBX.DHA-ICS-CYBER-RMF@HEALTH.MIL.

COMPLETION OF THIS QUESTIONNAIRE IS APPLICABLE TO REGULATED MEDICAL SYSTEMS/DEVICES AS WELL AS NON-REGULATED TECHNOLOGIES SUPPORTING THE MEDICAL MISSION.

PRIMARY VENDOR POINT OF CONTACT (POC) INFORMATION (Vendor Account Manager)		
Name:		
Job Title:		
Company:		
Business Address:		
E-Mail Address:		
Phone Number:		
Web page Address:		
Account Manager POC Signature and Date: (Signature indicates acceptance that all provided information is accurate, and that no information has been omitted.) If Digital Signature is not possible, print and sign this page only. Attach scanned copy to the document.		DATE:

VENDOR TECHNICAL POINT OF CONTACT (POC) INFORMATION (Technical POC Responsible for conducting RMF Activities)		
Name:		
Job Title:		
Company:		
Business Address:		
E-Mail Address:		
Phone Number:		
Web page Address:		
Technical POC Signature and Date: (Signature indicates acceptance that all provided information is accurate, and that no information has been omitted.) If Digital Signature is not possible, print and sign this page only. Attach scanned copy to the document.		DATE:

Section 1: System Identification

MEDICAL DEVICE AND EQUIPMENT IDENTIFICATION – Technical and Regulatory		
1.0 Medical Device/Equipment Title/Version: Provide the naming convention for the medical device/equipment and primary application version.		
1.1 Medical Device Description: **Provide a brief technical description of the medical device's/equipment intended use/capability. If applicable, the FDA 510K Summary Description should be used for accuracy.**		
1.2 Medical Device/Equipment Model: **List all devices/equipment and versions covered under this review (eg. family of systems)**		
1.3 Medical Device/Equipment Alternate Name: Indicate whether the medical device/equipment is marketed by any other model, brand names, trademark, or product suite/family. (eg. Resellers)		
1.4 Medical Device/Equipment Category: Recommend use of ECRI Institute's Universal Medical Device Nomenclature System (UMDNS).		
1.5 Primary Software Application Release/EOL Date: Provide the software release and expected End of Life (EOL) dates of the Primary Software Application. Also, indicate whether Extended Support for the Primary Software Application is provided by the manufacturer. See DHA Cybersecurity Acquisition Language	Release Date:	EOL Date:
1.6 Food and Drug Administration (FDA 510K)/other Regulatory Certification, or Premarket Authorization identifier, if applicable: Provide the number associated with the medical device/equipment, if applicable.		
1.7 Medical Device/Equipment Contract **Include in submission a copy of any existing purchase orders (PO), or contracts associated with a DoD/DHA purchase.** **If not yet sold to the DoD, indicate N/A.**	EXISTING CONTRACT/PO ATTACHED IN SEPARATE DOCUMENT:	
1.8 Department of Defense (DoD)/Defense Health Agency (DHA) Authorization: *State whether the proposed medical device/equipment has been, or is currently undergoing the DoD/DHA Risk Management Framework (RMF) Authorization process, and the corresponding eMASS record identifier. State the originating office conducting the RMF efforts, as well as the Authorization Termination Date (ATD).*		ATD:
1.9 Baseline physical testing location: *Is a test lab is available at the manufacturer's facility for RMF Assessment.* *If such a system is available, provide complete street address as well as Test Lab POC.*	☐ Yes ☐ No	
1.10 Intended Mode of Operation: Select the intended mode of operation of the medical device/equipment.	☐ Standalone MDE operates in complete physical and logical isolation. Data communication interfaces and associated networking protocols, including legacy serial RS-232 are disabled, and not able to be enabled by hospital staff. ☐ Peer to Peer – Operates in logical isolation but requires the use of networking protocols or RS-232 serial data communications for host-to-host connectivity.	

	☐ Client/Server – Operates as a distributed application that partitions task or workloads between the service requester (client) and the service provider (server) using networking protocols. ☐ Web-based – Client-side application – Operates as a distributed application that requires the use of a client-side browser and locally installed applets to access the Primary Application. Applets must be digitally signed by the server. ☐ Web-based –Zero Footprint client-side application. Operates as a distributed application that does NOT require the downloading and installation of server-side software to access the Primary Application. This may also be referred to as Server-side rendered application. ☐ Host-based – Operates as a passive subsystem which requires connection a host computer to produce information. It may require the use of networking protocols. ☐ Cloud-based – Operates within a cloud-service environment ☐ Government Cloud Service Provider (eg. DISA, SPAWAR) ☐ Commercial, or Vendor provided Cloud Service Provider (eg. Amazon Web Service)
1.11 Cloud Offerings For all Cloud offerings, indicate if the cloud solution is FEDRAMP approved, or has been evaluated by DHA J6 and approved for DHA use. List data transferred to/from, or stored within the Cloud. Indicate if data is downloadable by patient, or shared with third parties. (All cloud communications components MUST be clearly defined in Section 2: Technical Information)	☐ Not Yet Evaluated ☐ No Cloud Components ☐ FEDRAMP Approved (APPROVAL #: ##########) ☐ DHA J6 ESA-BAD Approved (APPROVAL: # ###########) Cloud Data Information:
1.12 Intended Method of Implementation: Select the intended method of implementation of the proposed medical device/equipment.	☐ System comprises Hardware + Software + Firmware (traditional configuration) ☐ System is Software Only in a Physical Environment (requires hardware provided by the GOV) ☐ System is Software Only in a Virtual Environment (requires virtual environment) ☐ Virtual Environment (all required hardware) is provided by the Department of Defense/Defense Health Agency ☐ Department of Defense/Defense Health Agency must provide all Operating System/Database/Application Virtual Servers. ☐ Virtual Environment (all required hardware) is provided by the Vendor ☐ Vendor provides, and is responsible for the configuration all Operating System/Database/Application on Virtual Servers
1.13 Interfaces Describe how the device connects to the Local Area Network (LAN), or the intended mode for communications.	**CONNECTION TYPE:** ☐ Serial over RS-232 ☐ RJ-45 Networked ☐ Serial to RJ-45 Connection ☐ 802.11 Wireless ☐ USB ☐ Other (Specify Connection Type Below)
1.14 Connected Systems Describe the types of systems this will connect to, or communicate with. (i.e. PACS, Networked patient monitors, Stand Alone, EHR, etc.) Indicate whether the MDE can support full/partial integration into a Microsoft Active Directory (AD) Domain.	

Section 2: Technical Information

2.0 SYSTEM HARDWARE/FIRMWARE
List all components required for the operation and clinical functionality of the device, to include all servers, workstations, routers, switches, etc. Any 3rd Party components MUST be indicated, and included in the tables, OR have their own MDERA filled out.

SYSTEM CONFIGURATION MUST BE DESCRIBED IN ITS ENTIRETY. FAILURE TO DISCLOSE ALL INFORMATION MAY CAUSE A BREACH OF CONTRACT.

Component	Purpose	Country of Origin	Comments
Ex: Console	Ex: Primary user interface	USA	Ex: Connected to the DoD

2.1 OPERATING SYSTEMS
For each Component Listed in Section 2.0, List the Operating System (OS): Make sure to identify all instances regardless of platform (i.e. server, client, peer, standalone, and portable peripheral end point device), End of Life (EOL) date and intended operational environment (i.e., physical, virtual)

EACH COMPONENT FROM SECTION 2.0 MUST BE LISTED. FAILURE TO DISCLOSE ALL INFORMATION MAY CAUSE A BREACH OF CONTRACT.

Component	Operating System	Country of Origin	Service Pack Level	End of Life Date	Extended Support	Virtualized
	Windows 10	USA				No

2.1.1 PROPRIETARY OPERATING SYSTEMS
For each Component Listed in Section 2.1 that indicated a Proprietary Operating System, the vendor MUST list the Underlying Technology used to develop the Proprietary OS:

Component	Operating System	Underlying Technology	Underlying Technology Version/SP	Underlying Technology EOL Date
Ex: Reconstruction Unit	Proprietary OS	RHEL	10	12/12/2023

2.2 INSTALLED APPLICATIONS
For each Component Listed in Section 2.0, List the Applications required for the System to operate/meet clinical requirements. Make sure to identify all instances regardless of platform (i.e. server, client, peer, standalone, and portable peripheral end point device), End of Life (EOL) date and why the software is required.
EACH COMPONENT FROM SECTION 2.0 MUST BE LISTED. FAILURE TO DISCLOSE ALL INFORMATION MAY CAUSE A BREACH OF CONTRACT.

Component	Application	Version	End of Life Date	Country of Origin	Purpose
Ex: Console	Primary Application	1.x	04-2022	USA	Primary Application used

2.3: MIGRATION PATH
For any Application, or Operating System (including underlying technology EOL) listed above, with less than 24 months of support/extended support, describe the migration plan, or upgrade path to maintain compliance.

2.4 Individually Identifiable User Accounts:
For each Component Listed in Section 2.0, describe the account types that are required for the system to operate. Are individual accounts for clinicians required for the application.
EACH COMPONENT FROM SECTION 2.0 MUST BE LISTED. FAILURE TO DISCLOSE ALL INFORMATION MAY CAUSE A BREACH OF CONTRACT.

Describe how accounts are created (site setup accounts, vs vendor default) List all account types in the table below:

Component	Account Type	Admin Account?	Application, OS, or DB?	Authentication Method (PKI, UN/PWD, etc.)	Purpose
Ex: Console	Clinician Account	No	Application	Username/password	Individual accounts

SYSTEM ARCHITECTURE DRAWING:

2.5 Medical Device Architecture Diagram: Provide a block diagram depicting all subsystems and components of the proposed medical system/device as configured in your proposal. Include connection specifications such as: Ethernet Connection, Wireless Connection or Bluetooth Connection. You may include an embedded Microsoft Visio diagram with your submission. All 3rd party components MUST be clearly identified in the architecture drawing.

2.6 END POINT PROTECTION - ANTI-VIRUS / HOST BASED SECURITY SYSTEM (HBSS) / HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS)

a. Provide a summary describing if 3rd party/Government Furnished applications can be installed on the proposed medical device/equipment. (i.e. Antivirus, HBSS, monitoring agents (SPLUNK, TANIUM, etc.)

b. If validation is required prior to installation, describe the validation process.

c. If the system does not support these applications, does the system utilize a native White Listing program (or other technology) to effectively mitigate the vulnerabilities associated with not supporting End Point Protection?

a.

b.

c.

	YES	NO
Anti-virus/Anti-malware recommended best practices (if available) **List items which must be excluded from scanning below.*	☐	☐
Antivirus/Antimalware Heuristics scanning supported?	☐	☐
Does the system provide notification of malware detection in the device user interface or through other mechanism (describe below)?	☐	☐
Does the system automatically update malicious code protection mechanisms? (If no, describe below how malicious code protection mechanisms are updated)	☐	☐

2.7 – VULNERABILITY SCANNING POLICY

Indicate limitations for the ability to run vulnerability scans (i.e. Nessus/ACAS/STIG scans) against the device.	
MDE can be scanned in a test/vendor lab environment only.	
No scanning capability at all (Serial/no networking capability)	
MDE can be scanned in a live environment	

Provide a summary describing if Network Vulnerability scans can be run against the device while in a live environment, and any limitations to the ability to scan the device in real time. (i.e. restrictions on running scans while conducting a study, system must be "de-hardened" and coordinated with the vendor prior to scanning, etc.).
If the MDE cannot be scanned in a live environment, but can be scanned in a vendor test lab, describe in detail the limitations to scanning within the live environment. (Impact to patient safety, etc.)

For devices that cannot be scanned in a live environment, provide detailed instructions as to how the MTF/DoD are to test for compliance, and verify the installed system is within the RMF authorized configuration. Failure to have testing methods for the device may result in a RMF authorization being revoked, and a Denial of Authorization to Operate (DATO) issued.

	YES	NO
Are admin account passwords made available to the local IT departments to facilitate Fully Credentialed Scans?	☐	☐

2.8 - VULNERABILITY MANAGEMENT/PATCHING POLICY

Provide a summary describing the plan for providing validated software updates and patches throughout the life cycle of the medical device/equipment. Include timeframes to approve patches, if critical OS patches can be installed without vendor permission. The summary should describe how the security patch is validated and then installed (e.g. remote installation by the vendor or distribution by the vendor for biomedical personnel at the healthcare organization to install.) The vendor should also specify the frequency of product updates.

2.9 REMOTE ACCESS

The software that provides the remote access capability must be included in the Application Inventory. Examples of remote desktop software applications are Microsoft Remote Desktop (MSRDP) and Secure Shell (SSH)	Yes	No
Can the medical device be serviced remotely (i.e., through the use of a secure point to point encrypted network connection)	☐	☐
Can the device be configured to require the local use to accept or initiate remote access?	☐	☐
Does the device provide an explicit indication of use to users physically present at collaborative computing devices?	☐	☐
Does the device require unrestricted access to the Internet in order to provide remote access?	☐	☐

2. 10 WIRELESS CAPABILITIES

(IEEE 802.11)

State whether the medical system/device employs any form of wireless communication, either standards-based and/or proprietary to facilitate the transmission/reception of data between system components and/or other systems?	Yes	No
Does the system employ wireless communication?	☐	☐
Wireless Mode of Operation ad hoc? (eg. Device connects internally to another wireless system component)	☐	☐
Wireless Mode of Operation infrastructure? (eg. Device connects to a LAN Environment)	☐	☐
Wireless Mode of Operation inherently disabled? (eg. Network adapter disabled in BIOS)	☐	☐
Wireless Authentication Method (eg. PKI, User-name/Password, Token)		
Wireless Encryption Method (eg. AES-256 CCMP)		

IEEE 802.15 BLUETOOTH
(Wireless Personal Area Network – WPAN)

Use FIPS 140-2 validated cryptographic modules for data in transit, including digital voice communications.	☐	☐
Bluetooth Discovery Mode Turned Off by default.	☐	☐

WIRELESS – Other (Describe any other wireless capabilities, i.e. Ultrawide band, Zigbee, etc.)			
Wireless Technology	Range (ft.) (indoor/outdoor)	Throughput (Mbps)	Purpose

2.11 – MASS STORAGE

Provide a summary describing if the use of USB Flash Drives/External Hard Drives is required for the operation of the system. Are drives required for use by the operator, or administrative in nature? Please detail what information is stored on the drives, how information on the drives is protected, and alternatives to using the drives. Indicate whether this information can be protected from unauthorized disclosure using Data at Rest (DAR) Full disk encryption.

2.11.1 USB Flash Drive

Upgrades/patches perform by? Vendor ☐ Customer ☐ N/A ☐	Yes	No
Upgrades /patches provided via USB by Vendor.	☐	☐
If the USB is provided by the Vendor, the USB flash drive is scanned and is free of malware prior to delivery.	☐	☐
If the USB is provided by Vendor, the USBs only contains the specific patch/upgrade data required for the device.	☐	☐

Section 3: Data Processing Capabilities

SYSTEM IDENTIFICATION – Data Processing, Electronic Protected Health Information / RMF Authorization	
3.0 Data Processing Capabilities: Does the proposed medical device/equipment perform any of the following data processing functions? (check all that apply)	☐ Receive ☐ Process ☐ Store ☐ Transmit ☐ Display
3.1 Electronic Protected Health Information/Personally Identifiable Information (ePHI/PII): (as defined by HIPAA Security Rule, 45 CFR Part 164) Indicate whether the proposed medical device acquires, processes, stores, displays/routes ePHI.	☐ Yes ☐ No
3.2 Non ePHI/PII information Define any data processed that is not ePHI/PII information.	
3.3 Electronic Protected Health Information/Personally Identifiable Information (ePHI/PII) Elements: (as defined by HIPAA Security Rule, 45 CFR Part 164) Identify each and all applicable ePHI elements.	☐ Address ☐ Dates of Birth, Admission, Discharge, Death, and all ages over 89 [and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older] ☐ Social Security Number ☐ Telephone numbers ☐ Fax number ☐ E-Mail address ☐ Medical Record Number ☐ Health Plan beneficiary number ☐ Account number ☐ Certificate/License number ☐ Any vehicle or other device serial number ☐ Device identifier or serial numbers ☐ Web Uniform Resource Locator (URL) ☐ IP address ☐ Finger or voice prints ☐ Photographic/Radiographic images ☐ Test Results ☐ Physiologic data with identifying characteristics ☐ Biometric data ☐ Personal Financial Data ☐ Any other unique identifying number, characteristic, or code.
3.4 DoD Information Persistence/Electronic Protected Health Information/Personally Identifiable Information (ePHI/PII) storage method: Describe the persistence of the DoD Information processed/stored/transmitted on or by the system.	☐ Permanently ☐ Temporarily **3.4.1 Specify how long/much data is stored, and what the method is used to remove data from the device. i.e. FIFO, Upon Reboot, etc..**
3.5 Data Input Method Describe the data input method. Distinguish between manual versus "prescribed" (automated/programmed) data input methods.	
3.6 Data Workflow Indicate what data elements enter the MDE, and what data elements leave the MDE. Indicate how data is processed and, or changed by the MDE.	

SYSTEM IDENTIFICATION – Data Processing, Electronic Protected Health Information / RMF Authorization	
3.7 Data At Rest Encryption Capabilities Describe any capability to encrypt data at rest. Include Encryption method and key strength (i.e. Bitlocker, AES-256)	
3.8 Data in Transit Encryption Capabilities Describe any capability to encrypt DoD Information/ePHI/PII while in transit. Include Encryption method and key strength (i.e. AES-256)	
3.9 USB Flash Drive Mass Storage (if available) USB flash drives for mass storage is provided by	Vendor ☐ Customer ☐ N/A ☐
3.10 USB Flash Drive Exporting (if available) USB flash drives for data export is provided by	Vendor ☐ Customer ☐ N/A ☐