**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<br>☐ Software<br>☐ Client<br>☐ 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)<br>*Please include OS build level.*<br>*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<br>☐ 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<br>☐ HTTPS<br>☐ TLS (version: _____)<br>☐ SFTP<br>☐ None<br>☐ 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)?<br><br>*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)<br>☐ 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<br>☐ Yes - VA S2S VPN<br>☐ Yes - VA Citrix<br>☐ Yes – VA Azure Virtual Desktop<br>☐ 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<br>☐ VHA-provided<br>☐ Other - describe<br><br>☐ Physical server<br>☐ Virtual host<br>☐ Cloud virtual host |
| 2.23 | If server-based, list server specifications (cores, RAM, power, storage) and rack space.<br>*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<br>☐ Results<br>☐ Billing (DFT)<br>☐ ADT<br>☐ 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?<br><br>*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<br>NSR Number: |
| | If no, to which security authorization boundary will this device/system be added?<br><br>*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<br>☐ MedMod Zone 6B<br>☐ MD-LITE<br>☐ Other _____ |
| | If no, what is the proposed EHR connection(s)/integration(s) type(s)?<br><br>*For additional guidance, please contact the EHRM IO HTM team at EHRMIOHTM@va.gov.* | ☐ Openlink (HL7)<br>☐ Compass Router (DICOM)<br>☐ EHR Gateway (Non-DICOM Image Routing)<br>☐ Cerner Connectivity Engine (CCE)<br>☐ CCE Terminal Server (CCE-TS)<br>☐ Separate HL7 Interface/Middleware Server<br>☐ None<br>☐ 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.*