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	Application Name and Software Version #	
1.5	Requesting Service	
1.6	VISN	
1.7	Facility Name	
1.8	Facility Number	
1.9	Manufacturer Point of Contact	
	Phone Number	
	E-mail address	
1.10	Biomedical Engineering Point of Contact	
	Phone Number	
	E-mail address	
1.11	Responsible Service if Biomedical Engineering is NOT the Primary System Manager for system maintenance, support and lifecycle management	
1.12	Medical Device Type	☐ Discrete device ☐ Software ☐ Client ☐ Application server
1.13	Equipment Description (i.e. equipment function and systems it communicates with)	
1.14	MDIA VLAN Number for installation (if known)	
1.15	Installation Location (Room, Building, Division)	
1.16	Is there an existing Enterprise Risk Analysis (ERA) for this device/system?	☐ Yes ☐ No
	If yes, what is the ERA number?	
	***Note that the ERA must be for the same make, model, and application software version to apply to the requested system. 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 system, 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 system and forward the document to either the Area Manager or ISSO for signature, as appropriate.		

2.1	Device Operating System (OS)	
	Can the OS be automatically patched?	☐ Yes ☐ No
	***Note that systems that do not support automated patching via the VHA MD Update Server 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?	
Procurement of systems 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 manufacture).		
2.2	Is the network connection wireless?	☐ Yes ☐ No
	If yes, what is the FIPS 140-2 certification number?	
Procurement of systems using 802.11 wireless networking that are not FIPS 140 2 compliant is prohibited.		
2.3	Does the device include a database?	☐ Yes ☐ No
	If yes, what is the database version?	
2.4	Can the device run McAfee antivirus?	☐ Yes ☐ No
	***Note that systems 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?	

2.5	For Windows-based devices, can the VHA SMAK toolkit be installed?	□ Yes □ No □ 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 systems that do not support SMAK installation or for which the vendor does not agree to provide a complete software inventory impose a significantly higher risk to the VA network.*	
2.6	Does the system support the use of two-factor authentication (please review the VA's requirements for two-factor authentication here)?	□ Yes □ No
2.7	Is the device required to be joined to the VA domain?	□ Yes □ No
2.8	Does the device allow for encryption of the data drive or OS drives?	□ Yes □ No
2.9	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
2.10	Will sensitive data be stored outside of the VA network (e.g. cloud-based service provider – excludes Electronic Medical Record connection)?	□ Yes □ No
2.11	Is connectivity external to the VA required for system operation?	□ Yes □ No
2.12	Is connectivity external to the VA required for system support?	□ No □ Yes - VA S2S VPN □ Yes – Other □ Yes - VA Citrix
	Describe remote access method and ports required if access is not via VA site-to-site VPN or VA Citrix.	
2.13	How many IP addresses are required?	
2.14	What kind of IPs does the system use?	□ Static IP □ DHCP
	***Systems should be deployed with static IPs unless DHCP is required.*	
2.15	If server-based, select one of the following:	□ Vendor-provided physical server □ Vendor-provided virtual host □ Biomedical Engineering-provided physical server □ Biomedical Engineering-provided virtual host □ OIT-provided virtual host □ Other – describe
2.16	If server-based, list server specifications (cores, RAM, power, storage) and rack space.	
2.17	Validate Cerner CareAware connection.	

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 Security Division (SDSD) to initiate the ERA process.*