

VA Medical Equipment Pre-Procurement Assessment

(*Indicates field is completed by Biomedical Engineering)

| | |
|--|---|
| *Equipment Category (VA-MDNS): | *Vendor: |
| *Requesting Service: | *Model: |
| *Requestor: | Vendor Contact: |
| *Installation Location: (Room-Bldg-Division): | If server based, specify rack space and power requirements: |
| *Biomedical Engineering Point of Contact: | *MDIA VLAN Number for Installation: |
| *Equipment Description (i.e., layman's description of equipment function and systems it communicates with): | |
| *If Biomedical Engineering is NOT the Primary System Manager for system management and maintenance, please note the responsible department below. Other | |

VA DIRECTIVE 6550
APPENDIX A

Medical Device /System Configuration

| | | |
|--|-------------|-----------------|
| What OS and version/Service Pack does the system utilize (e.g., Win7- SP1, Win Svr 2008, Linux)? | | |
| Does the system use a database application to operate? | Yes | No |
| If yes, specify which application/version: | | |
| Membership in the facility's Windows Domain is: | | |
| Required | Recommended | Not Recommended |
| | | N/A |
| Is a desktop web browser required to access the medical system/application? | Yes | No |
| If yes, specify which browsers and versions are supported: | | |
| If yes, does it require the use of https: and the VA SSL certificates – explain below: | | |
| If a browser is required, does it require a specific version of Java? | Yes | No |
| If yes, specify the version: | | |
| Is ActiveX required for client operation? | Yes | No |
| If yes, specify configuration requirements: | | |
| If Windows based, can the system use the National Medical Device Update Server for OS patches? | Yes | No |
| If no, specify how OS patching will be accomplished: | | |
| Can critical and routine OS and system security patches be applied as they become available without prior vendor approval? | Yes | No |
| If no, specify how approval notification to VA will be accomplished: | | |

**VA DIRECTIVE 6550
APPENDIX A**

| | | |
|--|-----|----|
| Can the device support the use of McAfee Anti-Virus (AV) software? | Yes | No |
| If no, what AV packages and versions are supported and describe the mechanism to provide updates. | | |
| Can USB ports be disabled on the device without compromising operation? | Yes | No |
| Can auto run be disabled for portable media? | Yes | No |
| Can VA install host-based security components such as a firewall, host intrusion prevention system (HIPS), anti-malware software, and/or any other security suite software required to operate on the VA production network? | Yes | No |

If “No” is the response to any of the above questions regarding updates and anti-virus software, please explain further for each item in the space below.

Authentication and User Account

| | | |
|--|-----|----|
| Is an administrator or power user account required to operate the device? | Yes | No |
| Can the device be made to require individual user authentication? | Yes | No |
| Does the device support password aging and strong user password accounts? | Yes | No |
| Does the device support auto logoff or/and session lock? | Yes | No |
| Does the system support the use of Active Directory for user authentication? | Yes | No |
| If yes, specify configuration requirements, LDAP etc.: | | |
| Does the system support the use of PIV/Smart Card only authentication? | Yes | No |

VA DIRECTIVE 6550
APPENDIX A

Data Handling

| | | |
|--|-----|----|
| Specify which Electronic Protected Health Information ePHI data elements are stored on the device (e.g., last name, SSN, DOB): | | |
| How many records with sensitive information can be stored on the device? | | |
| How long will they be retained on the device? | | |
| Is ePHI encrypted prior to transmission? | Yes | No |
| If yes, what is the encryption mechanism(s)? | | |
| What is the media used for long term storage? | | |
| How is data transmitted to the storage repository (e.g. LAN, DVD, USB, etc.)? | | |
| Is ePHI stored only on a drive partition or a separate drive to assist with end-of-life media sanitization? | Yes | No |
| Will the medical device require data backups? | Yes | No |
| If yes, specify how the system and data are backed up and what media is used: Describe backup process: (data centers are lights out so this needs to be known up front) | | |
| *Where will backups be stored and secured? | | |
| Does the device have the ability to assign unique ID numbers (accession numbers) instead of using patient identifying information (e.g., Social Security Number)? | Yes | No |
| If yes, how is it generated? | | |
| Does the device utilize a laptop for system operation? | Yes | No |
| If so, can the laptop be encrypted without impacting clinical functionality? | Yes | No |
| If yes, what encryption software can be used? | | |

Networking

| | | |
|---|-----|----|
| What are the LAN bandwidth requirements for full connectivity/performance? | | |
| What are the WAN bandwidth requirements for full connectivity/performance? | | |
| Provide a comprehensive list of all TCP and UDP ports that are required for operation: | | |
| Note: If more space is needed, please attach the comprehensive list of ports required for operation to this document. Attach a network diagram showing all communication requirements. | | |
| How many fixed IP addresses does the device require? | | |
| Is the device compatible with IP V6? | Yes | No |
| Vendors' products should be designed such that only ports required for the intended operation of the device are active. Are unused ports closed or disabled? | Yes | No |
| Can this be accomplished without impacting system operation? | Yes | No |
| Vendors' products should be designed such that only services required for the intended operation of the device are active. Are unused services (e.g., Telnet, IIS, etc.) disabled? | Yes | No |
| Can this be accomplished without impacting system operation? | Yes | No |
| Provide a comprehensive list of all services that are required for system operation: | | |
| Can the device be serviced remotely? | Yes | No |
| Does the vendor have an existing Site to Site (S2S) VPN tunnel or individual user VPN account(s)? | Yes | No |
| What remote access software does the system utilize (e.g., Dameware, PC Anywhere, etc.)? | | |
| Does the device require connection to the Internet to operate? | Yes | No |
| If yes, please justify and provide connection info (IP, port, protocol and traffic direction): | | |

VA DIRECTIVE 6550
APPENDIX A

Wireless

| | | |
|---|-----|----|
| Does the device utilize wireless communication? | Yes | No |
| <ul style="list-style-type: none">If yes, what protocols are used? | | |
| The encryption module must have FIPS 140-2 certification. Provide certificate number: | | |
| Are any ePHI data elements transmitted via the wireless link? | Yes | No |
| <ul style="list-style-type: none">If yes, list each element (e.g. last name, DOB, SSN). | | |

Integration with VA Healthcare Information Systems (if applicable)

| | | |
|--|-----|----|
| *Has the device been validated with VA's Clinical Procedures package? | Yes | No |
| *Has the device been validated with VA's Vista Imaging? | Yes | No |
| *Does the device have bi-directional HL7 interface? | Yes | No |
| List all other systems that the device will communicate with in order to operate properly, e.g. VistA, domain controllers, vendor's support network, etc.: | | |

Signature Page

| | |
|---------------------------------------|----------------|
| *Equipment Category (VA-MDNS): | Vendor: |
| *Requesting Service: | *Model: |

Chief, Biomedical Engineering
Concur/Non-Concur

Date

Chief Information Officer
Concur/Non-Concur

Date

Information Security Officer
Concur/Non-Concur

Date