VA Enterprise Design Patterns
Privacy and Security

Medical Device Security

OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)

VERSION 1.0
DATE ISSUED: JANUARY 2017

APPROVAL COORDINATION

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2017.02.22 15:14:25 -05'00'

Gary Marshall
Director, Technology Strategies, ASD

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2017.02.22 15:41:17 -05'00'

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Approver	Notes
1.0	1/20/2017	Nicholas Bogden	Updates addressing stakeholder feedback and Section 508 Compliance.

CONTENTS

1 Introduction 4
1.1 Business Problem 4
1.2 Business Need 5
1.3 Business Case 5
1.4 Approach 6
2 Current Capabilities and Limitations 7
2.1 Medical Device Procurement Requirements 7
2.2 Manual Application to the Security Architecture 8
2.3 Limited Visibility into Medical Device Activity 8
2.4 Disparate Management of Networked Medical Device Information 9
3 Future Capabilities 9
3.1 Build Security into New Medical Device Procurements 11
3.2 Secure the Network for Medical Devices 13
3.3 Enable Risk Management Through the MDPP 16
3.4 Medical Device Decommissioning 19
3.5 Alignment to the One-VA Technical Reference Model (TRM) 19
3.6 Alignment to Veteran-Centric Integration Process (VIP) 20
4 Use Cases 20
4.1 Medical Device Security 20
4.1.1 Purpose 20
4.1.2 Assumptions 20
4.1.3 Use Case Description 21
4.2 Networked Medical Device Support 21
4.2.1 Purpose 21
4.2.2 Assumptions 21
4.2.3 Use Case Description 21
4.3 Medical Device Critical Vulnerability 22
4.3.1 Assumptions 22
4.3.2 Use Case Description 22
Appendix A. Scope 24
Appendix B. Definitions 25
Appendix C. Acronyms 28
Appendix D. References, Standards, and Policies 30
Appendix E. MDPP Overview and Accomplishments 32

Table 1: Business Benefits 6
Table 2: Mapping of Future Capabilities of Business Problems 10
Table 3: List of Approved Tools and Standards for Medical Device Security 19

Figure 1: Medical Device Security Example with Data Fusion for Risk Management 18

Quick Jump

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

1 INTRODUCTION

The Department of Veterans Affairs (VA) has many devices that are used in patient healthcare for life support, diagnostics, monitoring, treatment, therapy, and analytics. VA designates a device as a medical device if it is Food and Drug Administration (FDA) certified or if it is connected to a medical device in a manner that can have a negative impact on patient safety if modified.[1] Many of these devices are certified through the FDA Premarket Review Process which inhibits the ability to install agents and perform patching to reduce security risks. This means that VA does not modify medical devices without written permission from the device manufacturer. The networking of medical devices provides many benefits for information sharing and data analytics, but also poses security risks to both the data and device integrity that must be addressed. This Enterprise Design Pattern (EDP) will address opportunities to enhance VA's ability to manage the inherent risk posed by medical devices. This document is designed to inform project teams that are responsible for the future development of medical device security programs. The goal is to support enterprise planning for medical device security that unites the various projects under a single vision and technical strategy as part of the continuous improvement process.

1.1 Business Problem

[1] See VA Directive 6550 for the official VA definition of a medical device.

VA created a comprehensive security initiative called the Medical Device Protection Program (MDPP) to manage the security of medical devices which is described in further detail in Section

Part of this program is the implementation of a Medical Device Isolation Architecture (MDIA) which isolates network connected medical devices in Virtual Local Area Networks (VLANs) with restricted Access Control List (ACL) communication profiles. Current challenges to the existing MDPP include:

- Medical devices which do not support cyber security requirements or enterprise management solutions
- Medical devices with longer lifetimes that run into end of support issues for software components while the device is still in use leaving vulnerabilities that cannot be patched
- Lack of information security standards to guide medical device procurements
- Inability to ensure medical devices are always segregated to minimize risk
- Lack of visibility into medical device network activity to identify changes to the risk profile
- Lack of robust asset management to efficiently support the tracking of medical devices for advanced risk management
- Lack of robust asset management to efficiently support the tracking of medical devices for advanced risk management

1.2 Business Need

VA has been cited by the VA Office of Inspector General (OIG) for deficiencies in the MDPP, such as weak network segmentation, as part of the Federal Information Security Modernization Act (FISMA) Material Weakness. VA Chief Information Officer (CIO) has set a goal to resolve the Material Weakness by 2017. As VA continues to see cyber security incidents affecting medical devices, establishing guidance for medical device security will help stakeholders to understand:

- What security requirements to consider when procuring new devices
- How to properly protect medical devices at the moment they are plugged into the network
- How to quickly identify and prioritize medical devices to enable risk management that considers both security and patient risks
- How to monitor and manage medical devices

1.3 Business Case

The goal of the Medical Device Security EDP is to:

- Improve the security of medical devices as part of the procurement of new devices
- Provide a more reliable network security architecture than the current MDIA
- Provide visibility into medical device activity and anomalies in network behavior
- Improve the efficient identification of networked medical devices to enable prioritized risk management

TABLE 1: BUSINESS BENEFITS

Business Benefits	Description
Improve the security of medical devices as part of the procurement of new devices	Provides incremental improvements in medical devices as inventory turns over. The device is the primary security weak point.
Provide a reliable network security	Reduce reliance on staff to properly identify medical devices and manually move them into a
Provide visibility into medical device activity and anomalies in network	Provides greater protection not only against cyber threats, but misuse and device errors.

1.4 Approach

The Medical Device Security EDP defines an enterprise medical device security model that addresses all phases of the medical device lifecycle. It starts with the assessment of medical devices procured, continues with the protection and risk management of devices on the network, and concludes with the disposal of the device. This model will help stakeholders meet VA security requirements for medical devices and avoid integrity and availability issues due to compromise. This EDP will:

- Review areas of IT risk for new medical devices
- Define an approach for protecting vulnerable medical devices connected to the enterprise network
- Describe strategies for ongoing risk management of medical devices with longer lifetimes than other network devices

2 CURRENT CAPABILITIES AND LIMITATIONS

VA continues to be a leader in medical device cyber security and is consulted by other federal, private, and international healthcare delivery organizations about the current program and future strategy. Since 2009, VA has had a robust MDPP that was created to help maintain the safe and effective operations of more than fifty-five thousand network-connected medical devices. For more information on the VA MDPP, please see Appendix E.

The medical device lifecycle begins with the procurement of the devices. Each facility initiates procurement of new medical devices using enterprise risk reviews performed for medical devices meeting certain criteria. Device owners must profile device security and the required communications based on the Manufacturer Disclosure Statement for Medical Device Security (MDS2) and information provided by the vendor. Once the devices are procured, they are entered into the Networked Medical Device Database (NMDD). Devices then go through a change control process and are placed into the MDIA VLANs to segregate them from other networked devices. At end of life for a device, device owners are responsible for reporting the disposition of medical devices for tracking purposes and meeting all compliance requirements for disposal.

While the current MDPP has made significant progress in reducing medical device information security risks, the evolving landscape continues to pose new challenges as described in the following sections.

2.1 Medical Device Procurement Requirements

VA Directive 6550, *Pre-Procurement Assessment for Medical Device/Systems,* provides current security policy on networked medical device procurements. It describes the technical pre-procurement assessment (PPA) requirements for medical devices. The PPA includes a comprehensive six-page questionnaire of over 50 questions for each vendor's device under consideration.

Device owners can use the MDS2 form provided by the vendor to help answer questions. However, the MDS2 form consists of basic "yes" or "no" answers and doesn't provide the level of detail necessary to answer many of the questions on the PPA, leaving the requestor to probe other documentation or contact vendor support to find answers. With the exception of Federal Information Processing Standard (FIPS) 140-2 compliance, the PPA does not establish a target minimum baseline for medical device security capabilities. Between the limitations of the MDS2

and open-ended nature of the PPA, the device owner may find it difficult to compare multiple devices side-by-side. This results in a reduced ability to weigh alternatives while factoring in information security.

2.2 Manual Application to the Security Architecture

MDPP created the MDIA architecture to isolate medical devices from the rest of the VA network to reduce the number of medical device malware infections. However, moving devices into the MDIA is a labor intensive process of identifying all ports, protocols, and communication paths, and turning those into ACLs to apply them to the network appliances. In 2010, it took seven months for the HISD to coordinate with the field to isolate many medical devices behind VLANs to meet MDIA guidance. Despite this effort, audits have identified ongoing challenges with medical devices outside the MDIA or ACLs that are not properly implemented.

The current design of the MDIA VLANs puts a heavy administrative burden on local support staff to create and maintain secure ACLs. The MDIA Rule Set contains 5 pages of instruction for creating rules. The MDIA design also adds to the processing overhead on the current network infrastructure. Due to the possible variations in each ACL, auditing the MDIA is also a highly manual process as it takes approximately a year to perform continuous monitoring of all ACLs in use. A lack of automation increases the risk of human error and reduces the ability to scale the solution as needed.

2.3 Limited Visibility into Medical Device Activity

The MDIA is designed to use VLANs to isolate medical devices and restrict communications to only those required for functionality. Communications are restricted based on source, ports, and destination. Due to the design of the VLANs, network traffic routed to a destination outside the VLAN is visible, but traffic between hosts within the VLAN is not. While the VLAN approach has been effective in some regards, it poses some challenges:

- In the past, this design has led to infections spreading from one medical device to another within the VLAN. This can pose a significant risk to threats such as ransomware, which tend to search for network peers to target.
- Medical devices are not necessarily protected when the destination is outside the VLAN either. The network traffic must cross an Intrusion Prevention System (IPS) for analysis to occur and IPS systems are only located at certain egress points across the enterprise. If traffic is encrypted, the IPS protection could be evaded.

- Finally, the MDIA operates at the network layer and does not provide protection at the application layer. This creates gaps in the visibility and monitoring of medical device network traffic. Visibility into medical device communications is important for identifying threats and mitigating any risk.

2.4 Disparate Management of Networked Medical Device Information

VA currently hosts over 50,000 networked medical devices that require enhanced protection. VA uses the NMDD for the purposes of helping to catalog technical attributes of medical devices. This information is manually entered by Biomedical Engineering, whose role as part of Health Technology Management (HTM) is the management of medical technology at VA.

VA also uses the SolarWinds monitoring and management solution to perform mapping of Media Access Control (MAC) addresses to Internet Protocol (IP) addresses. Biomedical Engineering is responsible for manually auditing the NMDD against SolarWinds data to identify any gaps. Enterprise vulnerability scanning generates a separate report on medical devices based on IP addresses which MDPP personnel and Biomedical Engineering must audit monthly to identify medical devices at risk.

This approach creates several challenges. Personnel must manually analyze multiple data sources to determine the current state of the medical device. Dynamic Host Configuration Protocol (DHCP) and changing IP addresses can create tracking problems. The NMDD does not ingest all data to become a single source providing comprehensive information on a medical device and its current risk profile. When a security incident involving a medical device is identified, the type of device (Life Supporting, Diagnostic, etc.) and vulnerability information may not be immediately available for use in assessing the severity of the incident.

3 FUTURE CAPABILITIES

Medical device security is an area that has continued to advance over the last several years at VA. The MDPP has been successful at reducing medical device infections and therefore mitigating risks to patient safety which is always the primary objective. As the MDPP continuously improves, there are already new projects in development which may relate to the areas listed below. Some of those projects include VA expectations and specifications for a strategy on common cybersecurity features, capabilities, and settings for network connected medical devices that can be provided to manufacturers. Another is integration of vulnerability reporting with the medical device inventory.

There are also new challenges as the MDPP grows and more medical devices migrate into the MDIA. VA must scale the design of the future medical device security approach to meet VA needs for managing high risk devices on the network that ultimately impacts the integrity of patient safety.

Medical device security must strike the right balance between reducing risk and protecting availability. Medical devices provide significant benefits to patient care, but already face increased risk of adverse events due to malfunction and human error.[2] Cybersecurity should limit further risk by preventing unintentional or malicious changes to the device while helping to detect potential errors. However, the MDPP must be careful not to introduce new risks, such as the adverse event reported to FDA where an antivirus client caused a medical device to fail during a cardiac catheterization procedure.[3]

Executive sponsorship is critical to driving increased collaboration between the Office of Information and Technology (OI&T) and the Veterans Health Administration (VHA) to combine the technical strategy and clinical expertise needed to support effective use of medical devices in achieving positive patient outcomes. As medical device technology changes and becomes more complex, the following section will highlight critical areas for review and provide guidance for providing a consistent approach for securing medical devices across VA networks. This guidance is designed to build upon the existing MDPP and support an enterprise approach to its continued maturation.

TABLE 2: MAPPING OF FUTURE CAPABILITIES OF BUSINESS PROBLEMS

Business Benefits	Description
Align Medical Device Procurement Strategy to Network Security	The procurement process provides guidance on security requirements to maintain existing network security and close identified gaps, when possible.
Increase Automation Around Network Security Architecture	Provides a network security architecture that employs a policy approach that limits administrative overhead to support the ability to scale the solution.
Increase Visibility Into Medical Device Activity	Network security solutions enable the ability to monitor communications both between medical devices and the rest of the VA network.

[2] http://nursingworld.org/.../Safe-Use-of-Devices.html

[3] https://www.accessdata.fda.gov/.../detail.cfm?mdrfoiid=5487204

Business Benefits	Description
Improve Identification of Medical Devices	Asset management centralizes information on medical device attributes including function, criticality, state, and location.
Improve Ability To Mitigate Varying Levels Of Medical Device Risk	Network security enables the ability to set policy based on the acceptable level of risk for individual medical devices.
Improve Risk Management Focused On Patient Care	Provides guidance on identified risks involving medical devices to facilitate the efficient use of related data to inform stakeholders to make decisions in support of

3.1 Build Security into New Medical Device Procurements

While legacy medical devices pose a challenge given the inability to update them to meet enterprise security requirements, newer medical devices provide an opportunity to consider security and enterprise integration from the beginning. As medical device procurements are initiated at the facility level, guidance in the form of policy and procedure is needed to ensure a consistent level of service delivery across VA.

Recommendations for Procurement of New Medical Devices

- **Establish Minimum Security Requirements:** While the current PPA Questionnaire gathers pertinent information, improvements can be made to make device comparison easier. Defining required security features at the beginning of the process will allow facilities to compare devices side by side using more quantitative analysis. This includes acceptable wireless networking services. Two growing wireless protocols for small devices include ZigBee and Bluetooth. Researchers hacked Internet of Things (IoT) devices that used Zigbee[4] due to a weakness in the protocol design. Some configurations of Bluetooth such as Low Energy (LE) are also susceptible to attacks,[5] which demonstrates the importance of standards for new devices. This may reduce the number of policy exceptions required for new medical devices.
- **Support Centralized Management:** The same medical device should not be deployed with varying software versions and configurations across different facilities at VA. This

[4] http://fortune.com/2015/08/07/zigbee-hacked/
[5] https://lacklustre.net/bluetooth/

increases security risks and the complexity of problem resolution. Prioritize medical devices that support centralized monitoring and configuration management.

- **Reduce Risk through Key Features:** Some security features have a greater impact on managing risk related to medical devices. Below are some features that support network security and risk management:
    - **802.1x Support** – This provides authentication of the device when joining the Local Area Network (LAN) to aid in the identification and tracking of medical devices.
    - **Event Log Export** – Medical devices create event logs of audit activity, but the value is diminished if the logs cannot be exported. The FDA has already created draft guidance on sharing patient-specific information from medical devices.[6] Enabling centralization of this data can support multiple purposes including security monitoring, device health monitoring, clinical analysis, and Health Insurance Portability and Accountability Act (HIPAA) compliance. Vendor identification of logged error codes further enhances advanced device health monitoring.
    - **Device Integrity Enforcement** – While authentication can provide an initial barrier to unauthorized access, medical devices are more vulnerable to unauthorized access than typical IT assets due to the need to ensure the device is readily accessible for patient care. However, normal clinical use should not involve the modification of system or application software. Unintended modifications to the system could alter device functionality or the output data. Prioritize devices that support methods to maintain the integrity of the system.
    - **Encryption** – Legacy devices often do not support encryption. The increase in network connectivity of medical devices creates a risk for the compromise of sensitive data at rest and in transit. Even on a trusted network, devices are occasionally compromised and may intercept data on the LAN sent in cleartext. Prioritize devices with the ability to encrypt data at rest and in transit.
    - **Endpoint Security Solutions** – Legacy signature-based antivirus and host intrusion prevention suites are diminishing in their ability to block modern threats. Security suites that can whitelist allowed activity and block anomalies may present the lowest risk. Integration of this capability by the vendor is preferred to reduce the risk of false positives which can inhibit device functionality.

[6] http://www.fda.gov/downloads/medicaldevices/.../guidancedocuments/ucm505756.pdf

- **Establish Pre-Procurement Testing:** There is a need to validate each medical device profile including network communications and vulnerabilities before it is put into operations. VA has entered into a Cooperative Research and Development Agreement (CRADA) with Underwriters Laboratories to develop a process to certify the cyber security posture of medical devices. There is the potential for this process to result in testing that satisfies this requirement and provides an acceptable risk profile for devices that are certified. At this time, this process is still under development. Even when complete, there is the possibility that some procured medical devices may not be certified. When certification is not possible, VA still needs the ability to test medical devices for cyber security. Due to the cost of medical devices, creating an appropriate lab environment may be prohibitive. VA must develop procedures to safely perform a limited pilot in operations that results in comparable risk reporting. Testing should include the following:
    - **Network Protocols Used** – Validate all communications documented by the vendor with the expectation that everything else will be blocked.
    - **Use of Known Credentials** – The use of known or default credentials creates an easy method for attackers to access a device. IoT devices with known credentials contributed to one of the largest Distributed Denial of Service (DDoS) attacks to date.[7]
    - **Malware scanning** – A preventative scan to determine whether the device has shipped with malware installed.
    - **Vulnerability scanning** – In addition to identifying vulnerabilities, there is a known issue where some devices are designed to operate in a known state and will restart if the sequence of network communications is interrupted by a vulnerability (or any other) scan. These devices can still be scanned with proper coordination. Support for continuous scanning should be confirmed during testing, as opposed to device owners discovering a reset device later in production.
    - **Penetration Testing** – Test all means of communicating with the medical device to determine if malformed input or exploits can impact the device.

3.2 Secure the Network for Medical Devices

Procurement is only one area for enhancing medical device security. While newer devices may support better integration, legacy devices do not need replacement as long as they continue to

[7] https://www.us-cert.gov/ncas/alerts/TA16-288A

support patient care without creating a significant risk. Network security is the means by which to reduce the risk of legacy devices with known vulnerabilities to enable their continued use. In compliance with both National Institute of Standards and Technology (NIST) and the *Internet of Things (IoT) EDP* Section 3.2, use of a Device Isolation Architecture (DIA) is required and MDIA is one application of this concept. The following list provides guidance to improve network security while reducing the current administrative overhead:

- **Integrate Medical Devices with Network Access Control (NAC):** New medical devices should not be able to access the network without first entering them into the enterprise medical device Inventory. Although not all devices will support 802.1x or device authentication, every device can be entered into the inventory. This will reduce the risk by clearly identifying all devices and owners.
- **Migrate from IP and Port Based Rules to Policy-Based Rules** – The use of firewall rules based on the IP address and port creates additional administrative overhead and increased risk of implementation errors. It also requires the use of static IP addressing to manage endpoints. Migrate to a network security strategy that uses policy based on allowed application, device and user rules to reduce complexity and reliance on static addressing. Identifying devices through authentication, network profiling, and inventory enables the creation of policy based on groups or zones. As an example, a policy based strategy might operate in the following manner. The medical device is connected to the network. It authenticates to allow network access or its MAC address is used to whitelist its access. Device profiling may be used to ensure the MAC address is not spoofed. A static IP address is not required. The identification of the device aligns it to group policy in the application firewall. The medical device is a magnetic resonance imaging (MRI) machine. Devices in this group are allowed to communicate with the image repository server group. The policy restricts groups to specific application protocols. Anomalous traffic in violation of existing policy is flagged for investigation or blocked depending on the device profile defined in the asset management solution.
- **Enhance Visibility into Medical Device Activity:** There are multiple methods to increase visibility which are described below:
    - **Establish a Comprehensive Medical Device Asset Management Capability** – The medical device inventory should be comprehensive and capture both automated and manually entered information. As the volume of medical devices grows, limit manual interaction as much as possible to support scaling and data accuracy.
        - Network solutions are able to capture both static and dynamic information on medical devices such as the IP address, MAC address,

hostname, Operating System, Vendor, Model, Version, vulnerabilities, last authenticated user and alerts. Adding information on the criticality of the device's role in patient care, the device owner and technical point of contact can improve the speed of coordinated risk management.

- Record the FDA Unique Device Identifier (UDI) in the inventory to aid in linking logical information to physical devices as part of enhancing risk management.[8] There are multiple scenarios where the tracking of UDI in relation to other data may be beneficial. The UDI can be used to quickly track when specific medical device models have already been approved for VA use. The UDI can connect establish more reliable device identification for IT incidents. The UDI could also be helpful in identifying patients impacted by a medical device whose integrity was affected by an incident, if UDI information is also being recorded in patient electronic health records (EHR). Under the 2015 Edition Health IT Certification Criteria, implantable device UDIs have to be included as part of an EHR's Common Clinical Data Set (CCDS).[9] Tracking the UDI of devices providing diagnostic results included in EHRs could be beneficial as well. Please note that offices such as the VHA Department of Logistics are using solutions to track UDI information and integrate with VistA. Collaboration is required to ensure a single authoritative source for UDI tracking.
- Incorporate business requirements from other areas within VA that involve tracking information about medical devices. Some projects are working on equipment location tracking. Vendors and the FDA provide public notices around vulnerabilities, available updates and product recalls. Users may report specific scenarios of electromagnetic interference (EMI) or radio-frequency interference (RFI) degrading medical devices. The Joint Commission (TJC) requires tracking of some device maintenance and testing.[10] Centralizing this information can help all stakeholders.
- Change management is an important element of maintaining a comprehensive inventory. In coordination with the NAC solution, devices should be blocked from the network until they are fully entered into inventory and assigned an appropriate policy.

---

[8] http://www.fda.gov/MedicalDevices/.../UDIBasics/default.htm

[9] https://www.healthit.gov/policy-researchers-implementers/2015-edition-final-rule

[10] https://www.jointcommission.org/assets/1/18/Changes_to_AHC_Standards.pdf

        - It is also possible to use inventory data to perform data analytics with real-time information to create a risk score or alert level for each medical device. Health Technology Management (HTM) should review whether the existing inventory solution can support this level of functionality.
    - **Leverage Local Network Monitoring Solutions –** As part of the Continuous Diagnostics and Mitigation (CDM) effort, VA is deploying other solutions across the enterprise. Medical devices must be added to the scope of these solutions and to enhance the MDPP by performing passive network monitoring, device discovery, and device profiling where possible.
    - **Perform Network Security at the Application Layer** – Attackers will often exfiltrate data by tunneling data over open ports, such as port 80 or 443 using other protocols. Limiting network security to layer three and below reduces visibility and creates an avenue for exploitation. Communications between the MDIA VLANs should traverse a solution which performs application layer inspection of network traffic and enforces policy.
    - **Whitelist Allowed Communications and Block Everything Else** – In coordination with the enterprise medical device inventory, designate allowed network traffic and block everything else. Medical devices should not have unexpected configuration management activities or new protocols that suddenly begin communicating. HISD can use a pilot to profile network traffic for existing medical devices as part of managing transitional risk, but the end goal should be to prevent attackers' access to services not used by the medical device for patient care. Blocking intra-VLAN communications where not required will also help to ensure network traffic passes through network security solutions placed between the VLANs.

3.3 Enable Risk Management through the MDPP

Procurement policies and network security solutions provide the ability to enhance the controls for medical devices. Although this will strengthen security, collaboration between OI&T and VHA remains a critical piece of risk management for medical devices. The MDPP should be an ongoing discussion between the technical and clinical support teams to define the appropriate level of risk to deliver the best care to Veterans. The following areas can improve risk management via the MDPP:

- **Create Closer Collaboration between OI&T and VHA** – As visibility into medical devices is improved through enhanced asset management and data fusion, it can create

additional use cases. Health Technology Management and Health Information Security Division should include other stakeholders to assess the ability to use medical device data and metadata to improve patient care. This collaboration could be unified under a Medical Device Center of Excellence or similar construct to support continuous improvement among participants. This formalization is important to support collaboration between the organizations throughout staffing transitions.

- **Integrate MDPP Reporting with the National Center for Patient Safety (NCPS)** – The NCPS's goal is "the reduction and prevention of inadvertent harm to our patients as a result of their care." Medical devices certainly have the potential to harm patients when their integrity is compromised with unknown impact. When a data entry error results from having to manually transfer data from a device display to a chart, this can be difficult to trace unless the device data is available. It is much more difficult to trace an errant device output due to medical device compromise unless the compromise is known. Coordinating with NCPS can aid in correlating IT incidents to patient outcomes to track adverse events or "near misses."
- **Enhance Integration with Security Operations** – Medical device data fusion will be used to increase the effectiveness of the MDPP. This includes analyzing authentication data, Netflow data, application layer events, policy violations, security solution events, and the enterprise medical device inventory. While manually attempting to evaluate all these information sources simultaneously would be overwhelming, integrating this data with a Security Incident and Event Management (SIEM) or other data analytic solution, in accordance with the *Auditing Enterprise Design Pattern*, will allow stakeholders to more quickly visualize anomalies, identify risks, and coordinate with impacted parties for risk management.
- **Identify the Risk Profile of Medical Devices** – As mentioned in Section 3.2 under the recommendations for the medical device inventory, medical devices operate at varying levels of risk. This is based on their function, vulnerability, connections to other systems, and ability to be monitored. OI&T and VHA collaboration is important to agree on a system for assigning a risk profile to medical devices that can leverage security operations procedures.
- **Predefine Remediation Actions for Medical Devices** – By tracking the risk profile of medical devices, HISD can predefine remediation plans based on the device information. Non-critical devices may be quarantined to prevent the spread of malware to other devices, while more critical devices may only be monitored until risk management discussions can include clinical support staff. Definition of standard procedures should speed containment and prevent unintended interruption of patient care where possible.

- **Identify Vulnerabilities in Clinical Workflows** – Not all areas of exposure are identifiable through a vulnerability scan of the device. Processes and procedures can also create areas of risk for device compromise. Collaboration with VHA can help identify devices that require closer monitoring due to the operation and use of the device.

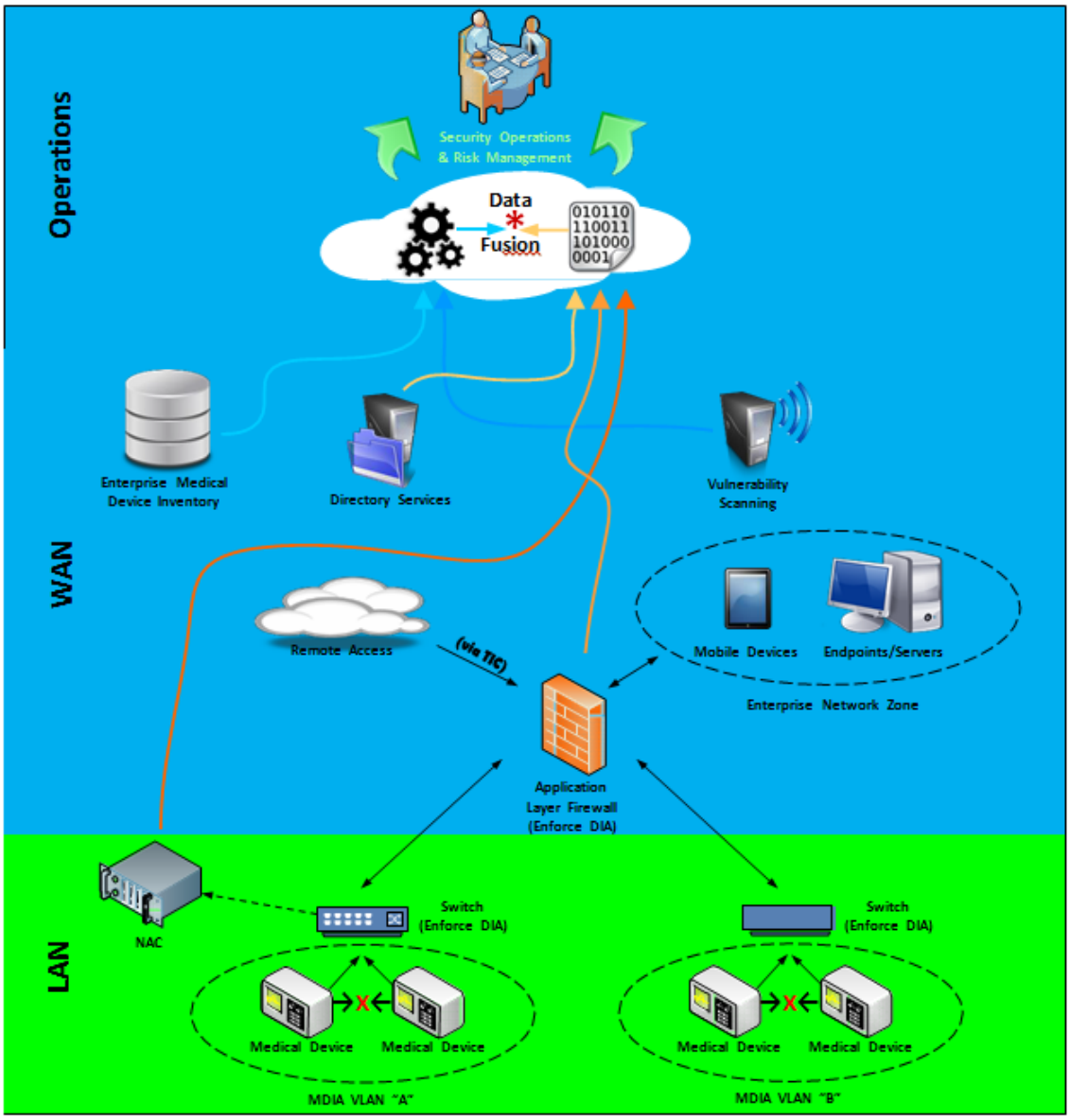

FIGURE 1: MEDICAL DEVICE SECURITY EXAMPLE WITH DATA FUSION FOR RISK MANAGEMENT

3.4 Medical Device Decommissioning

Local VA facility policy currently guides the disposal of medical devices in compliance with FDA and TJC requirements. As medical device asset management becomes a more integral part of risk management, connecting these local activities with the medical device inventory will improve visibility. There are two primary goals in doing so:

- Maintain an accurate inventory of active medical devices and their state
- Audit compliance with VHA Handbook 1605.03 and the secure disposal of any Protected Health Information (PHI) that exists on medical devices

3.5 Alignment to the One-VA Technical Reference Model (TRM)

All projects will leverage the approved tools and technologies located in the VA ONE-VA Technical Reference Model (TRM) to comply with the architectural guidance provided in this document.

The following table is a Summary of Recommendations which will address the limitations expressed in Section 2.

TABLE 3: LIST OF APPROVED TOOLS AND STANDARDS FOR MEDICAL DEVICE SECURITY

Technology	Example Technologies	Example Standards	Mandated ESS
Auditing	Qradar, LogRhythm, Splunk Enterprise Security	N/A	TBD
Authentication	SiteMinder, Active Directory	X.509, Oauth/OpenID Connect, Kerberos, SAML, Lightweight Directory Access Protocol (LDAP), 802.1x	Identity and Access Management (IAM) Access Services
Authorization	Axiomatics, DataPower	XACML, LDAP	IAM Access Services
Encryption	FIPS 140-2 compliant	WS-*, TLS per FIPS 140-2 requirements	N/A

Technology	Example Technologies	Example Standards	Mandated ESS
Monitoring	CA User Activity Reporting Module, ElasticSearch Logstash, Microsoft System Center Operations Manager (SCOM), Splunk, SolarWinds Log and Event Manager (Requested)	Syslog Protocol Internet Engineering Task Force (IETF) RFC 5424, Transport Layer Security (TLS) Transport Mapping for Syslog (IETF RFC 5425)	TBD

3.6 Alignment to Veteran-Centric Integration Process (VIP)

Veteran-centric integration (VIP) IP is a Lean-Agile framework that serves the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely, and predictably. VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

More information can be found here: https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/.

4 USE CASES

The following use cases are examples that demonstrate the application of the capabilities and recommendations described in this document.

4.1 Medical Device Security

4.1.1 Purpose

The purpose of this use case is to discuss how security requirements affect the medical device procurement process.

4.1.2 Assumptions

- All potential medical devices can meet the clinical requirements for patient care.
- Differences in cost are a factor, but not in scope of this use case.

- The vendor can provide all requested information.

4.1.3 Use Case Description

1. A Veterans Affairs Medical Center (VAMC) would like to procure a new medical device and needs to know if there are minimum security requirements.
2. The requestor contacts the local BME for guidance.
3. BME provides the requestor with the minimum security requirements for medical devices and instructions for requesting a risk review if all the requirements cannot be met.
4. The requestor provides a standard form to each vendor to gather all necessary information for a side-by-side comparison.
5. The requestor submits the preferred medical device along with a business justification and information on alternate products, if any.
6. HTM follows the updated VA Directive 6550 process for VHA networked medical devices to make a risk based decision on the best medical device for patient care. The assessment reviews data on suitability, cost, and security considerations.
7. HTM approves the procurement of the medical device. Any enhanced network security requirements are identified and initiated as part of the procurement process.

4.2 Networked Medical Device Support

4.2.1 Purpose

The purpose of this use case is to discuss how network security is designed to provide automated security for medical devices. This includes application of Device Isolation Architecture (DIA) principles.

4.2.2 Assumptions

- The medical device is normally inventoried and profiled in advance as part of the procurement and change management process.
- The medical device is authorized for access to the VA network.
- Wireless communication not using the VA network is out of scope.

4.2.3 Use Case Description

- An Infusion Pump has been recently procured and moved to a patient room. Staff need to know that network support is transparent and security maintained.

- The VAMC staff plug the device into the VA network jack in the patient's room.
- The medical device is not able to obtain network access. An alert is logged by the VA Network Security Operations Center (VA-NSOC) of attempted unauthorized physical network access. VA-NSOC contacts the VAMC to investigate the issue and confirms using the recorded MAC address that the Infusion Pump was the source of the alert.
- VA-NSOC coordinates with the HISD and Biomedical Engineering to confirm the Infusion Pump has not yet completed change management in order to be added to the network.
- Biomedical Engineering gathers the missing information for change management. Using the profile from existing Infusion Pumps, HISD and VA-NSOC coordinate quickly to complete the change management process and assign a network security profile to the new Infusion Pump.
- The VAMC staff plug the Infusion Pump into the network and confirm connectivity. The VAMC staff move the Infusion Pump to another room and plug it into the network jack. Network connectivity is confirmed and VA-NSOC confirms the network security profile has been automatically applied.

4.3 Medical Device Critical Vulnerability

The purpose of this use case is to discuss how network security is designed to provide ongoing protection for medical devices with vulnerabilities.

4.3.1 Assumptions

- The medical device is normally inventoried and profiled in advance as part of the procurement and change management process.
- The medical device is authorized to for access to the VA network.
- Wireless communication not using the VA network is out of scope.

4.3.2 Use Case Description

1. A significant vulnerability has been identified in an older medical device used by VA across many VAMCs and Community Based Outpatient Clinics (CBOC) which may not be updated by the vendor. Leadership has requested a report on the level of risk to continued use for patient care.
2. HISD quickly generates a report from the NMDD of all medical devices affected by the identified vulnerability.
3. HISD coordinates with VA-NSOC to determine what protections exist to mitigate the vulnerability.

4. VA-NSOC is able to implement detection of attempts to exploit the vulnerability at the network and application layer to provide protection until patches can be applied.
5. HISD summarizes all information and reports to leadership on the current level of risk to patient care.
6. HISD coordinates with Biomed to contact vendors and medical device remediation is prioritized based on the level of risk to patient care.

APPENDIX A. SCOPE

This EDP provides an enterprise-level view of the "As-Is" and "To-Be" mobile capabilities relevant to Veteran-facing mobile applications and the standard processes in use. The document will refer to, rather than duplicate, lower-level solution guidance associated with these capabilities.

A Medical Device Security Model sets standards for how network connected devices are assessed and integrated into the VA enterprise to maintain integrity for the sake of patient safety. This EDP will define an enterprise medical device security model that starts with the assessment of medical devices procured through the protection of devices used in operations. This model will help stakeholders to meet VA security requirements for medical devices and to avoid integrity and availability issues due to compromised devices. This EDP will include:

- A review of the areas of IT risk for new medical devices
- Strategies for connecting medical devices to the enterprise network
- Strategies for ongoing risk management of medical devices with longer lifetimes than other network devices

Topics that are out of scope for this EDP, but may be referenced, are:

- Network performance not related to security
- Physical security of devices within VAMCs
- Medical devices that leave the VA network
- IoT devices that are not medical devices

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA's OI&T, Enterprise Program Management Office (EPMO), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from VHA, Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Access	Interaction with a computer system for instance VistA. Such interaction includes data retrieval, editing (create, update, delete) and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, et cetera.
Accurate, unambiguous user identity	Information that represents the actual human that is interacting with a computer system, including the initiation of that interaction.
Application proxy	Construct involving the use of a generic, non-human "user" entity to represent "machine-to-machine" interaction where appropriate for interactions that do not involve a specific end user.
Auditing	The inspection or examination of an activity based on available information. In the case of computer systems, this is based on review of the events generated by the system or application.
Biomedical Engineering	The application of engineering principles and design concepts to medicine and biology for healthcare purposes (e.g. diagnostic or therapeutic).
Consuming application	The application consuming services from a provider system. Generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services.
Continuous Monitoring	The process and technology used to detect compliance and risk issues associated with an organization's financial and operational environment.
Delegated Access	When an owner authorizes another to serve as his or her representative for access to a particular resource.
Dynamic Host Configuration Protocol (DHCP)	A communications protocol that network administrators use to centrally manage and automate the network configuration of devices attaching to an IP network.

Key Term	Definition
Intrusion Prevention System (IPS)	A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
Manufacturer Disclosure Statement for Medical Device Security (MDS2)	A form that provides information about the security controls that are implemented in a medical device in order to protect the protected health information (PHI) transmitted or stored by the medical device.
Media Access Control (MAC)	A unique identifier assigned to network interfaces for communications at the data link layer of a network segment.
Medical Devices	is any instrument, apparatus, appliance, software, material, or other article whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application.
Medical Device Isolation Architecture (MDIA)	A risk management program where the architecture relies on virtual local area networks to help isolate the devices from the rest of the VA network.
Medical Device Protection Program (MDPP)	Manages the security of medical devices. Part of this program is the implementation of a MDIA.
Network Security Architecture	A unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls.
Pre-Procurement Assessment (PPA)	Assessment of medical devices and medical systems, prior to procuring medical devices that store sensitive patient that will be connected to the VA information network
Risk Management	The identification, assessment, and prioritization of risks followed by coordinated and application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.

Key Term	Definition
Solarwinds	IT monitoring and management tools are built for SysAdmins and network engineers who need powerful and affordable tools.
Virtual Local Area Networks (VLAN–)	A group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
ACL	Access Control List
ASD	Architecture, Strategy, and Design
BME	Biomedical Engineer
CBOC	Community Based Outpatient Clinics
CCDS	Common Clinical Data Set
CIO	Chief Information Officer
CRADA	Cooperative Research and Development Agreement
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DIA	Device Isolation Architecture
EDP	Enterprise Design Pattern
EMI	Electromagnetic interference
EPMO	Enterprise Program Management Office
ETA	Enterprise Technical Architecture
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HISD	Health Information Security Divis
HTM	Health Technology Management
IAM	Identity and Access Management
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol

Acronym	Description
MAC	Media Access Control
MDIA	Medical Device Isolation Architecture
MDISS	Medical Device Innovation, Safety and Security Consortium
MDPP	Medical Device Protection Program
MDS2	Manufacturer Disclosure Statement for Medical Device Security
MRI	Magnetic resonance imaging
NAC	Network Access Control
NCA	National Cemetery Administration
NCPS	National Center for Patient Safety
NMDD	Networked Medical Device Database
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
OI&T	Office of Information and Technology
PHI	Protected Health Information
PMAS	Project Management Accountability System
PPA	Pre-Procurement Assessment
SDE	Service Delivery and Engineering
SIEM	Security Incident and Event Management
SOA	Service-Oriented Architecture
TJC	The Joint Commission
TRM	Technical Reference Model
VAMC	Veterans Affairs Medical Center
VA-NSOC	VA Network Security Operations Center
VBA	Veterans Benefits Administration
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VLAN	Virtual Local Area Network

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing EDPs all VA projects developing IT systems in accordance with the VA's OI&T integrated development and release management process, the VIP.
2	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
3	VHA	VA Directive 6550	Describes the pre-procurement assessment requirements for medical devices and systems.
4	VHA	VA Handbook 1606.03	Privacy Compliance Assurance Program and Privacy Compliance Monitoring. Outlines requirements related to the safeguarding of sensitive information including disposal of records.
5	NIST	NIST SP 800-121	Guide to Bluetooth Security. Provides a description and recommendations around the various implementations of Bluetooth.
6	FDA	Federal Food, Drug, and Cosmetic Act (FD&C Act) United States Code Title 21	Parts 800-1299 of this code establishes FDA authority over medical device regulation and requirements related to identification, tracking, reporting and other areas to include 510(K) Premarket Approval (PMA).

#	Issuing Agency	Applicable Reference/ Standard	Purpose
7	FDA	Safe Medical Devices Act of 1990	Defined requirements to report device-related deaths and serious injuries to the FDA.
8	TJC	The Joint Commission Environment of Care	The Joint Commission is an independent, not-for-profit organization that accredits and certifies health care organizations and programs in the United States. Their Environment of Care program establishes standards for hospitals and laboratories which include the management of medical devices.

APPENDIX E. MDPP OVERVIEW AND ACCOMPLISHMENTS

VA's Medical Device Protection Program (MDPP) is based on collaboration between Office of Information Technology (OIT) Field Security Service (FSS) Health Information Security Division (HISD) and VHA Healthcare Technology Management (HTM) Program and was created to help maintain the safe and effective operations of more than fifty five thousand network-connected medical devices deployed in VHA medical centers and clinics. MDPP encompasses: (1) security guidance, training, and outreach to VA employees, contractors, and volunteers; (2) continuous monitoring of evolving cyber security threats, including ongoing impact assessments for changes made to medical device hardware or software; (3) configuration control to ensure security of VA networks and to verify medical devices are operating as the manufacturer intended; and (4) incident response to remediate security breaches and resolve vulnerabilities to medical technologies.

The MDPP has been successful with designing a defense-in-depth approach to securing medical devices. These devices will aid in countering cyber threats and mitigating vulnerabilities through application of twenty-three diverse sets of security controls (e.g., Risk Assessment, Pre-Procurement Assessment and MDIA) that contain specific policies and guidance that have been fully implemented. One of the strengths of the MDPP is that the cyber security strategy focuses on multiple layers of administrative, technical, and physical safeguards that work together to reduce the attack surface and minimize negative outcomes of compromise without inhibiting performance of the medical device or the patient's healthcare experience. This strategy engages medical devices throughout the system development life cycle (SDLC) so that security practices are aligned to each of the major phases.

The MDPP continues to improve medical device cyber security. In 2016, the MDPP collaborated with VA Biomedical Engineers (BME) to remediate more than 4,015 MDIA ACL configurations and there was an enterprise effort to remediate more than 300,000 medical device vulnerabilities. As a result of VA's cyber security efforts, medical device manufacturers are now seriously considering how to incorporate cybersecurity as part of the life cycle of medical devices. There are also several new MDPP projects in progress. There is a security posture document being developed which "establishes VA expectations and specifications for a strategy on common cybersecurity features, capabilities, and settings for network connected medical devices." This document will provide the VA's cybersecurity specifications for manufacturers. MDPP is also working with vulnerability management teams to integrate vulnerability scanning data into the NMDD inventory so that there are more accurate vulnerability reports and documentation of changes which were not approved by manufacturers.

The VA is a leader in medical device cyber security and is consulted by other federal, private and international healthcare delivery organizations about our accomplishments and strategy. The VA is a co-founder of Medical Device Innovation, Safety and Security Consortium (MDISS). MDISS is "a collaborative and inclusive nonprofit professional organization committed to advancing quality health care with a focus on the safety and security of medical devices. We serve providers, payers, manufacturers, universities, government agencies, technology companies, individuals, patients, patient advocates and associations. Our mission is to protect public health and well-being by advancing computer risk management practices to ensure wide availability of innovative and safe medical devices." MDISS provides a platform for interaction and discussion with other healthcare delivery organizations and manufacturers about medical device cyber security. One of those efforts is a tool that the VA helped develop that will automate the risk analysis of medical devices to provide a more consistent qualitative and quantitative output to guide procurement of medical devices.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.