Challenges to VA Information Protection in the 21st Century: Medical Device Security

Jaren Doherty
Acting Deputy Assistant Secretary,
Information Protection and Risk Management

August 4, 2010

Table of Contents

Veterans entrust us with their private information and expect world class patient care from the VA

- ***As the largest healthcare provider in the Federal Government, VA has:***

- ***7.84 million enrollees in the VA Healthcare System***
- ***153 medical centers***
- ***768 community-based outpatient clinics (CBOCs)***
- ***232 Veteran centers***
- ***Over 50,000 networked medical devices***

…VA must secure medical devices in order to maintain data integrity and prevent erroneous results that may negatively impact patient safety

VA currently faces critical challenges in securing medical devices from cyber threats

- ***Medical devices can restrict the application of operating system patches and malware protection updates, which can potentially cause:***
  - ***An increased vulnerability to malware attacks and potential to serve as an entry point for attacks into the trusted network***
  - ***A risk to patient safety and protection of patient sensitive information***

Photo Source: Department of Veterans Affairs

A **medical device** is defined as any device that:

•Is used in patient healthcare for diagnoses, treatment, monitoring of physiological measurements, or for health analytical purposes

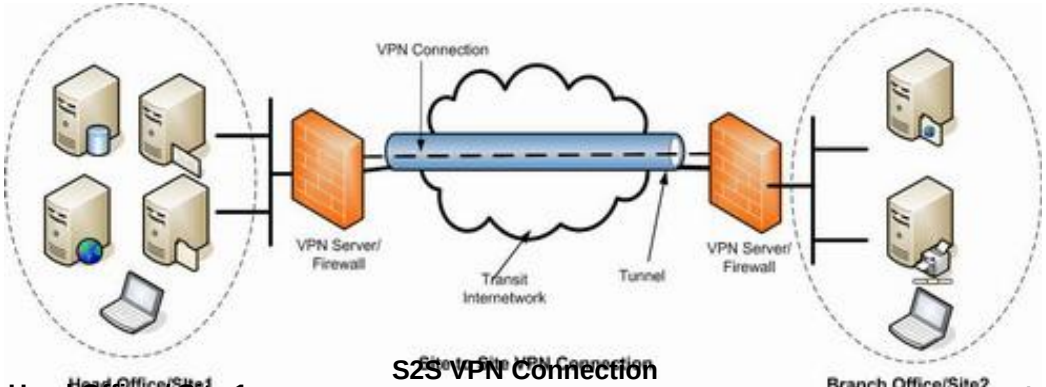
▪Has gone through the Food and Drug Administration's (FDA) Premarket Review Process

▪Is part of a medical device and, if modified, can have a negative impact on the functionality/safety of the main device

Table of Contents

To enhance security, VA requires medical device vendors to utilize a Site-2-Site (S2S) virtual private network (VPN)

- *An encrypted tunnel is created between the VA gateway and the vendor*
- *Vendor employees access VA resources through approved Internet Protocol (IP) addresses that have been added to the VA national firewall*
- *There is no individual authentication*
  - *However, the company is required to have a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA), Business Associate Agreement (BAA), and review and approval from the Enterprise Security Change Control Board (ESCCB)*
  - *The S2S can be local, Veterans Integrated Service Network (VISN), or national*



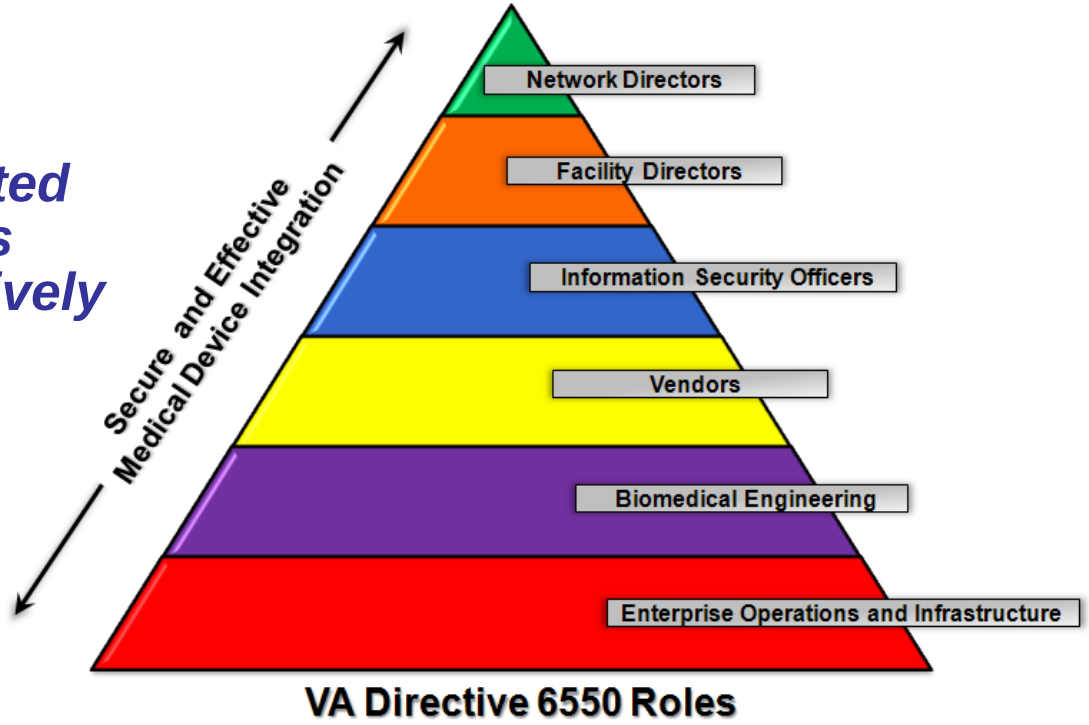
S2S VPN Connection

Head Office / Site 1 **VA Healthcare Center / Site 2**

Photo Source: Vermont Department of Information and Innovation

VA policy mandates networked medical devices and devices that store patient data to undergo a pre-procurement assessment

- *Per VA Directive 6550, 'Pre-Procurement Assessment for Medical Devices', performing a technical service assessment during the acquisition planning process:*
  - *Addresses risk*
  - *Assures medical devices are integrated with VA IT networks and systems effectively and securely*



VA Directive 6550 Roles

VA employs a six-step process using a virtual local area network (VLAN) structure to secure medical devices

1	2	3	4	5	6
Device Identification	***Grouping and Segmentation***	***Identify Communication Requirements***	***Migration Planning and Coordination***	***System Migration***	***Implementing Protection***
Create a Medical Device Inventory worksheet of all networked devices requiring isolation	Group devices in the Medical Device Inventory worksheet into systems/ modalities and assign these to VLANs	Identify what systems communicate with outside of the local VLAN	Identify workflow issues, connection stakeholders, and stakeholder change responsibilities	Transfer devices to the appropriate VLAN	Implement firewall rules between the medical device VLAN and external networks
Owner Primary: *Biomedical Engineering* Secondary: *IT Operations*	**Owner** Primary: *IT Operations* Secondary: *Biomedical Engineering*	**Owner** Primary: *IT Operations* Secondary: *Biomedical Engineering*	**Owner** Primary: *Biomedical Engineering, IT Operations, and Information Security Officers (ISOs)*	**Owner** Primary: *IT Operations* Secondary: *Biomedical Engineering*	**Owner** Primary: *IT Operations* Secondary: *ISOs*

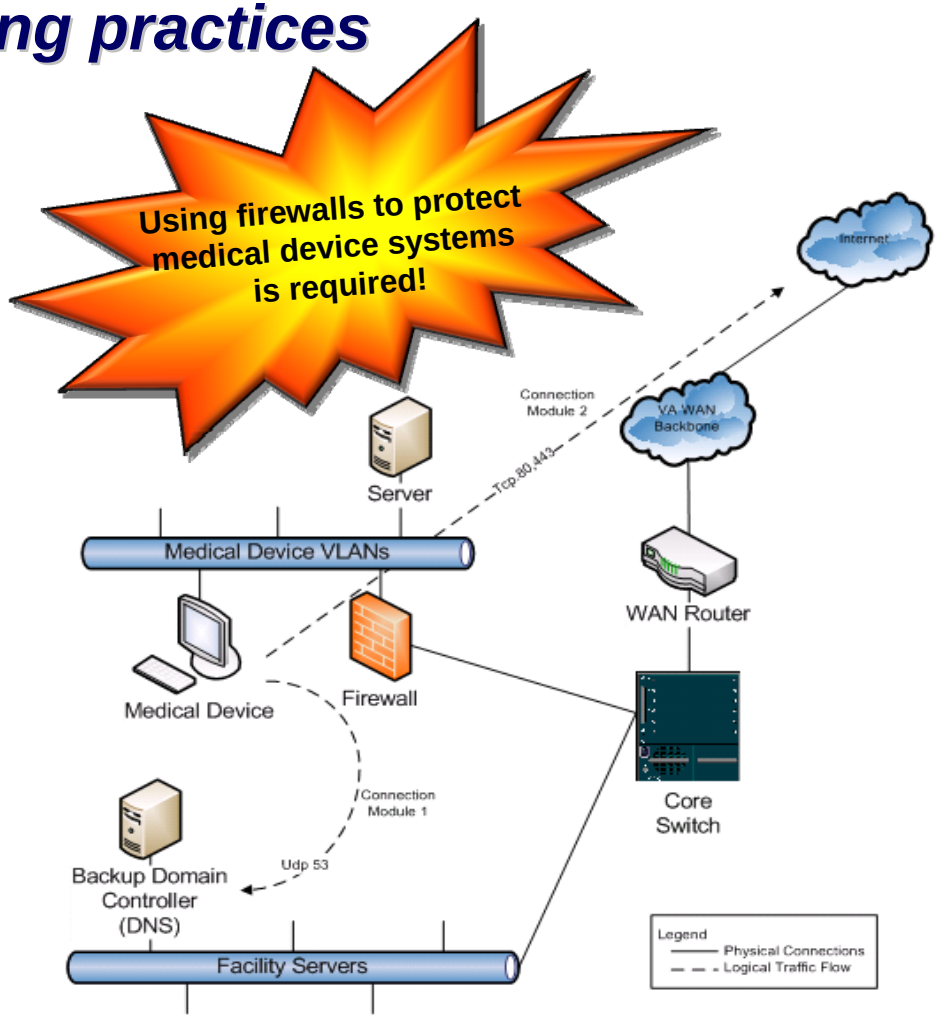
…this process should be applied to systems that are connected to the VA network but cannot be patched in accordance with VA patching policy

Firewalls allow medical devices to communicate while maintaining best security and networking practices

Firewalls provide stateful packet inspection and are hardened against attacks directed at them

Inbound firewall rule sets are applied to each Virtual Local Area Network (VLAN) interface coming into the firewall

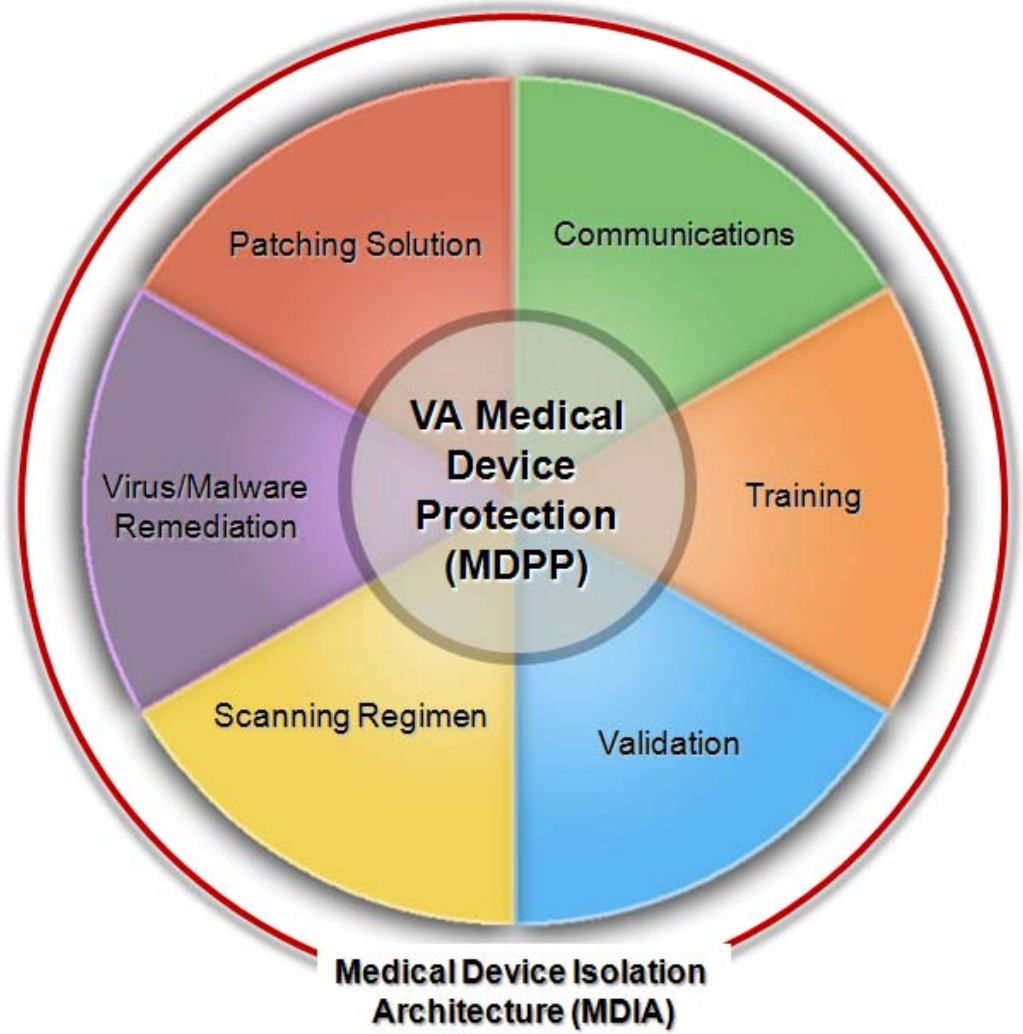
- ***Ensures that only allowed traffic from inside the VA network flows through the firewalls***
- ***Reduces the risk that medical device systems will be compromised***



VA MDIA

(Guidance established in 2004 and updated in 2009)

VA is simultaneously developing a comprehensive protection strategy for securing medical devices



VA's medical device protection strategy encompasses communications, training, validation…

Communications

- The Information Protection and Risk Management (IPRM) Office is utilizing memorandums, the IP Portal, the IP Update newsletter, and the Risk Management and Incident Response (RMIR) Office's "What If" newsletter to communicate MDIA information
- Field Security Operations (FSO) is meeting with ISOs, VA-NSOC, Biomedical Engineering, and IT Operations in every region, as well as other Federal agencies, to answer questions and ensure medical device security requirements are understood

Training

- FSO, with communications support from IPRM Communications, has developed MDIA role-based training (RBT) tailored to various parties – ISOs, VA Network Security and Operations Center (VA-NSOC), VHA Biomedical Engineering, and the IT community
- FSO has also created RBT on VA Directive 6550

Validation

- OI&T is developing an ongoing review process to validate implementation
- A monthly status report will be provided throughout the full deployment of the MDIA
- The IPRM Emergency Response Team (ERT), IT Office of Oversight & Compliance (ITOC), and Inspector General (IG) will ensure that VLANs are in place

…scanning, remediation, and patching

Scanning Regimen

- FSO is researching improved medical device scanning techniques in coordination with Veterans Health Administration (VHA) Healthcare Technologies Management (HTM) and the vendor community

Malware/Virus Remediation

- The Office of Information and Technology (OI&T) is creating a virus and malware strategy to enhance detection and eradication
- OI&T recommends that all medical devices be equipped with approved anti-virus protection
- Full cooperation from the vendor community is required to ensure full deployment of anti-virus protection

Patching Solution

- OI&T is initiating a more robust patching program for medical devices in coordination with VHA HTM and the vendor community
- A pilot to improve patch management and strengthen access control for isolated medical devices is in the planning stages; to include a repository of approved patches that will be made available to VHA Biomedical Engineers
- FSO met with FDA to determine actual restrictions relative to anti-virus and patching

Table of Contents

VA has made great strides in medical device security…

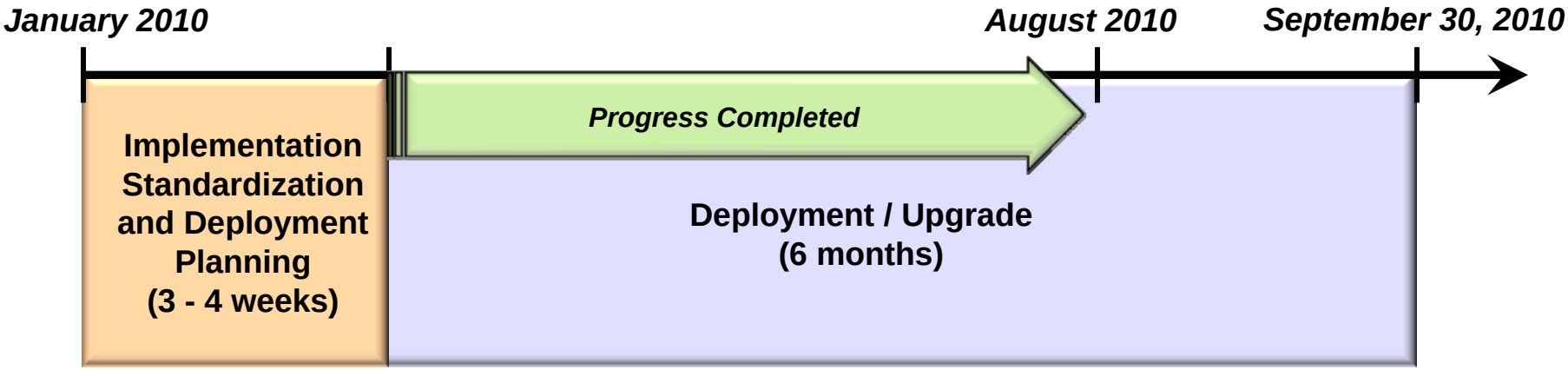
- Released a memorandum requiring medical center Facility CIOs to certify all medical devices are isolated within MDIA VLANs with approved Access Control Lists (ACLs) by September 30, 2010
- Administered MDPP and VA Directive 6550 RBTs to over 550 ISOs, VA-NSOC staff, IT Operations staff, and Biomedical Engineers
- Reviewed over 1,835 medical VLANs and assigned a grade rating level of effort required to bring MDIA into compliance with 2004 guidance
- Working on a secure patch repository for medical devices
- Developing a standard operating procedure (SOP) for medical device infection remediation
- Meeting monthly with the Department of Defense, Indian Health Service, and vendors to discuss medical device security issues

…just to name a few!

…but we still have a lot of work to do!

- *It will take approximately 7 months* to update existing Medical Device VLANs to meet the 2004 MDIA guidance*
- *This task will:*
  - *Require a concerted and organized effort*
  - *Bring VA into compliance with the baseline 2004 guideline one year from the release of the 2009 MDIA guidance*

PROPOSED TIMELINE



…once all Medical Device VLANs meet 2004 MDIA requirements, work will begin to reach compliance with the 2009 MDIA guidance

* Estimate

Questions?