VA Medical Device Protection Program (MDPP)

Presented to

National Institute for Standards and Technology (NIST)
Health Security Conference

VA INFORMATION PROTECTION

May 11, 2011

Table of Contents

VA INFORMATION PROTECTION

Achieving Security Takes Teamwork…

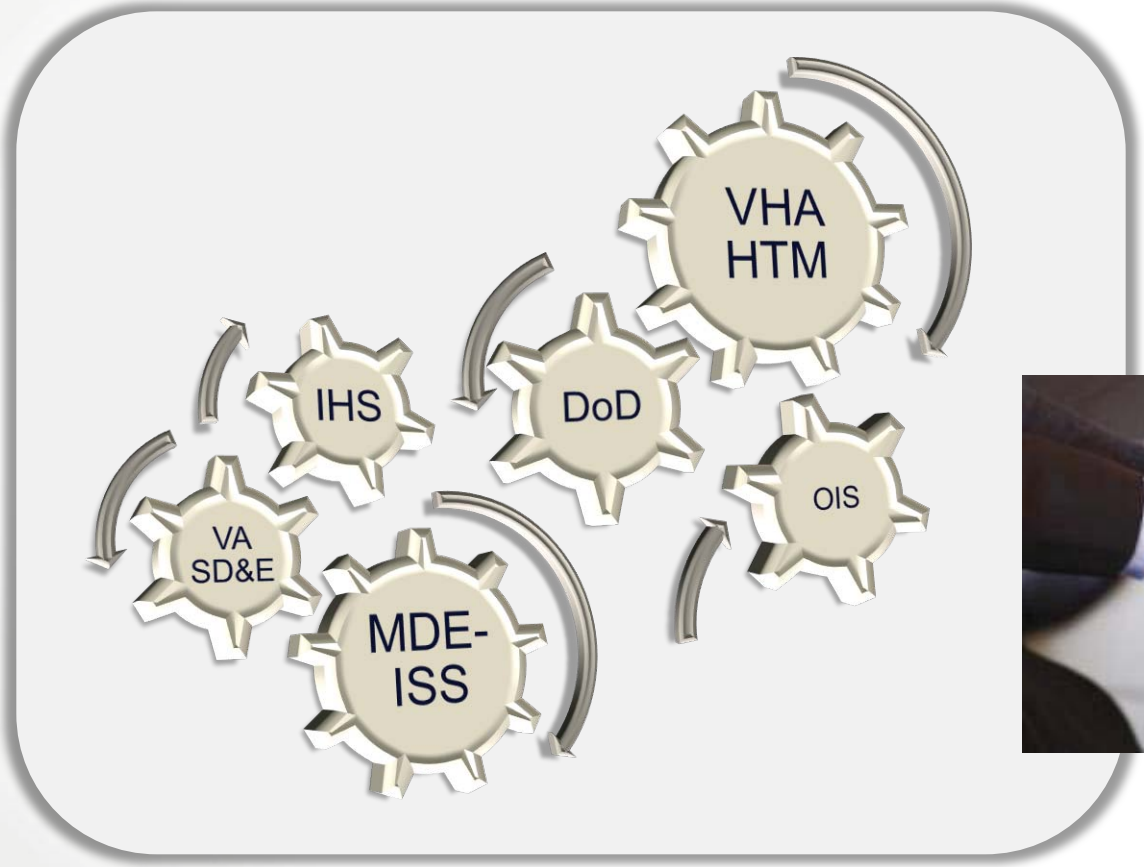


Photo Source: Idaho Department of Commerce

VA INFORMATION PROTECTION

Data Protection and Patient Safety are Critical VA Priorities

Photo Source: Department of Health and Human Services

"Any Personally Identifiable Information (PII) and electronic Patient Health Information (ePHI) that is collected, stored, or transmitted across medical device systems should be protected with the best possible security tools for the deployed systems."

– Health Information Portability and Accountability Act (HIPAA)

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

VA INFORMATION PROTECTION

Threats to VA Medical Devices

- 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 component(s) [hardware, software] that is/are:

- Food and Drug Administration (FDA) 510K certified;
- Any device that is used in patient healthcare for diagnosis, treatment, or monitoring;
- Any ancillary support device – including but not limited to external disk storage, database servers, gateway or middleware interface devices – that are required for the medical device to function properly.

Networked medical device: Any medical device that is connected to the VA network.

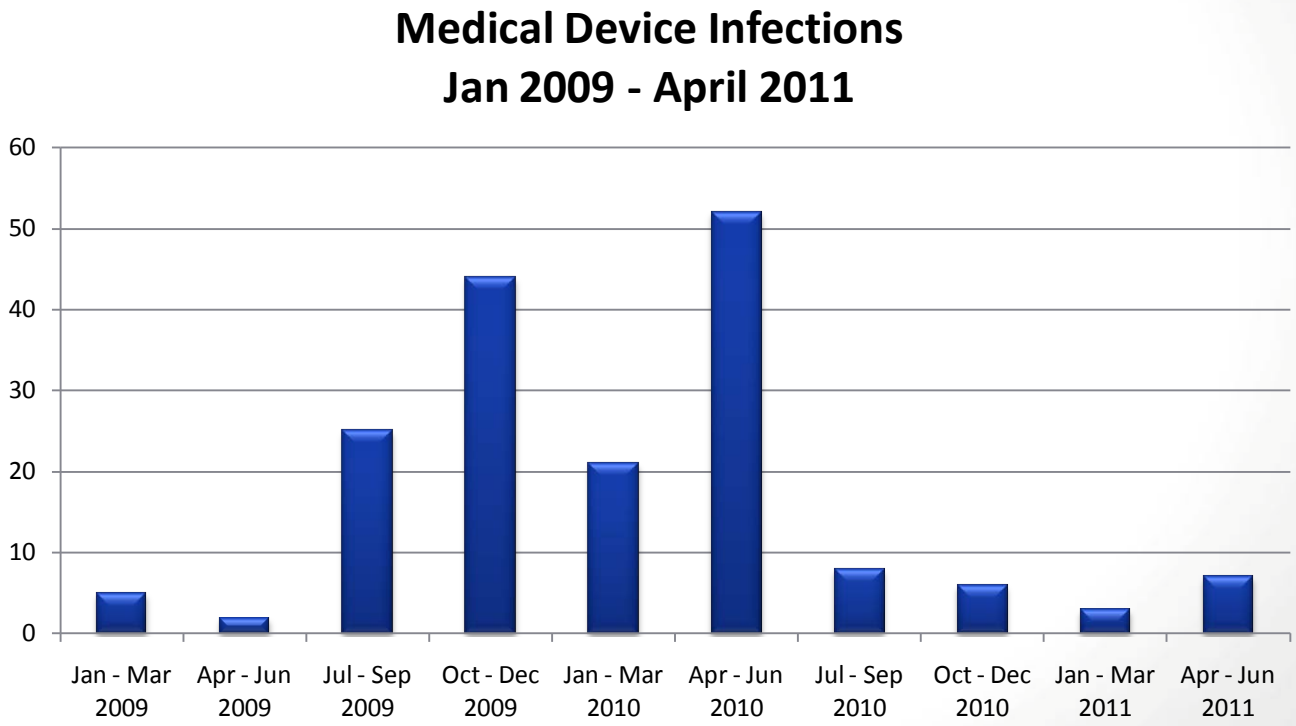
Networked medical system: Any group of devices that make up a complete medical system. These are multiple devices that are required for the medical system to function as intended by the manufacturer/vendor.

VA INFORMATION PROTECTION

Threats to VA Medical Devices…(con't)

- VA is tracking reported incidents on networked devices

*173 Medical Device Infections since January 2009



(Source: VA Network Security and Operations Center (VA-0NSOC) Weekly Threat Brief)

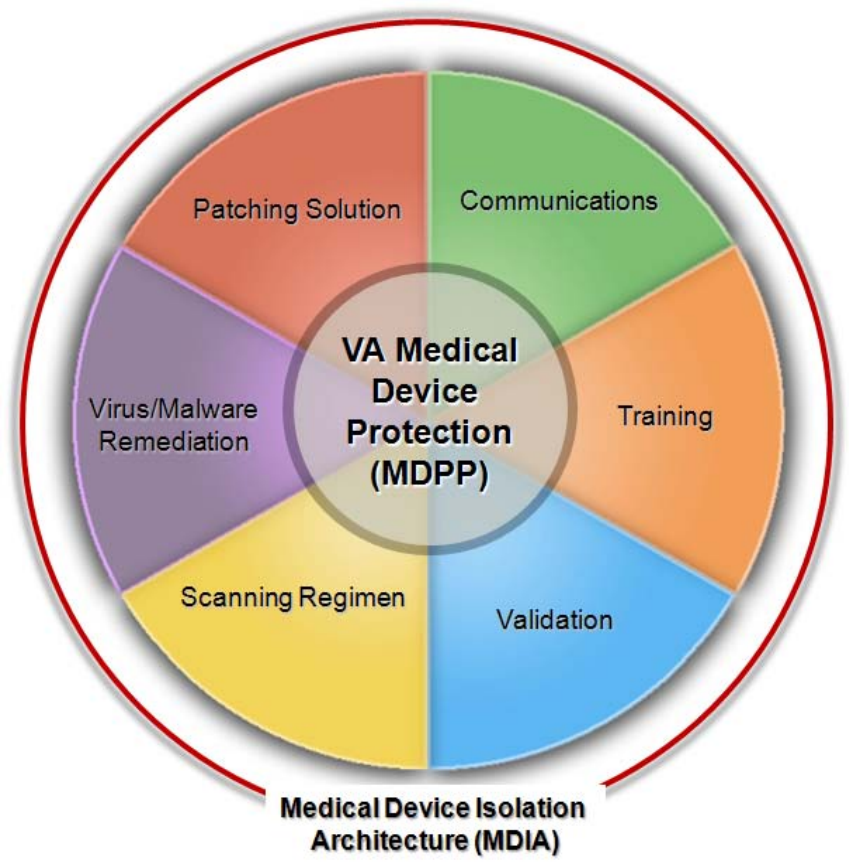
VA INFORMATION PROTECTION

Table of Contents

VA INFORMATION PROTECTION

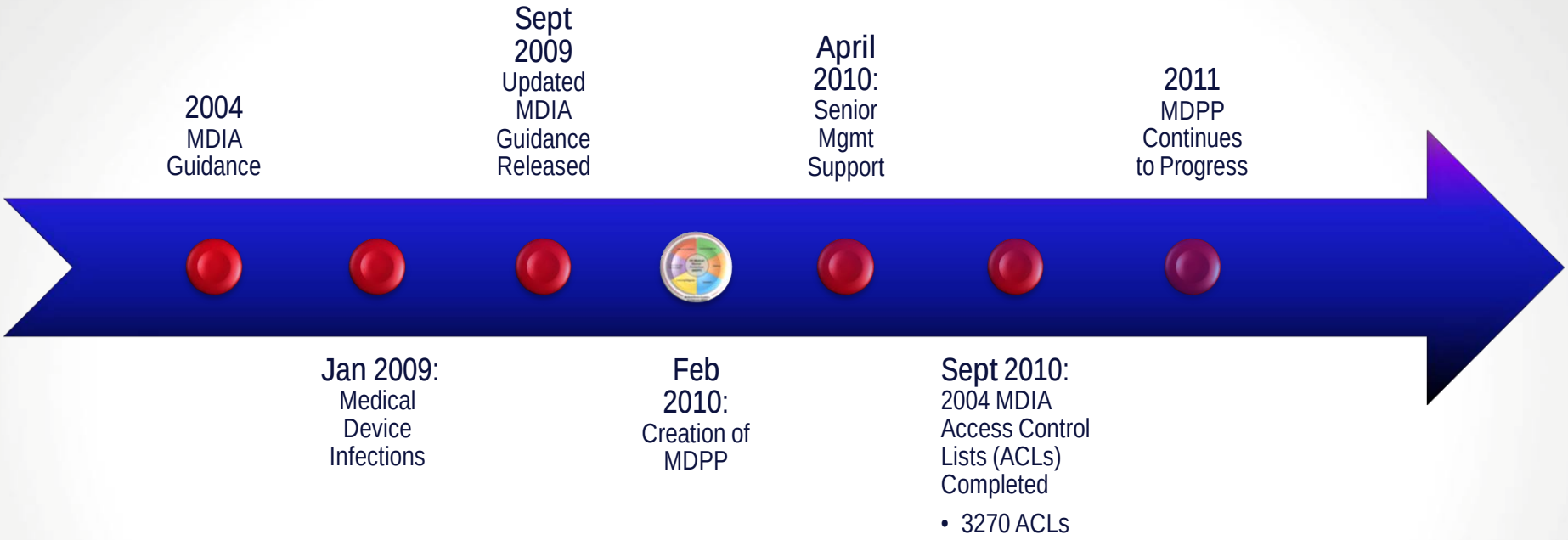
Medical Device Protection Program

- To better safeguard medical devices, VA developed a comprehensive security initiative that encompasses:
  - Communication
  - Training
  - Validation
  - Scanning
  - Remediation
  - Patching
  - Medical device isolation architecture (MDIA)



VA INFORMATION PROTECTION

MDPP Has Evolved Over Time

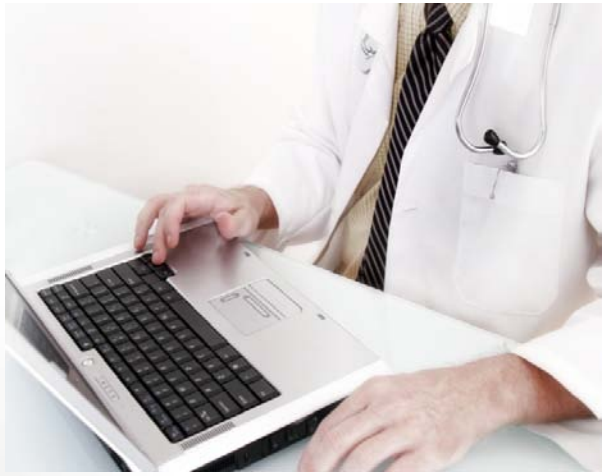


- MDPP has grown and changed over time to meet the challenge of evolving threats to VA medical devices
- The program will continue to grow and change to create a service oriented architecture that meets the needs of the organization and addresses the risks of medical devices

VA INFORMATION PROTECTION

MDIA Has Been Implemented VA-wide

- As of September 30th, 2010, approximately 50,000 medical devices have been isolated behind nearly 3,200 virtual local area networks (VLANs)

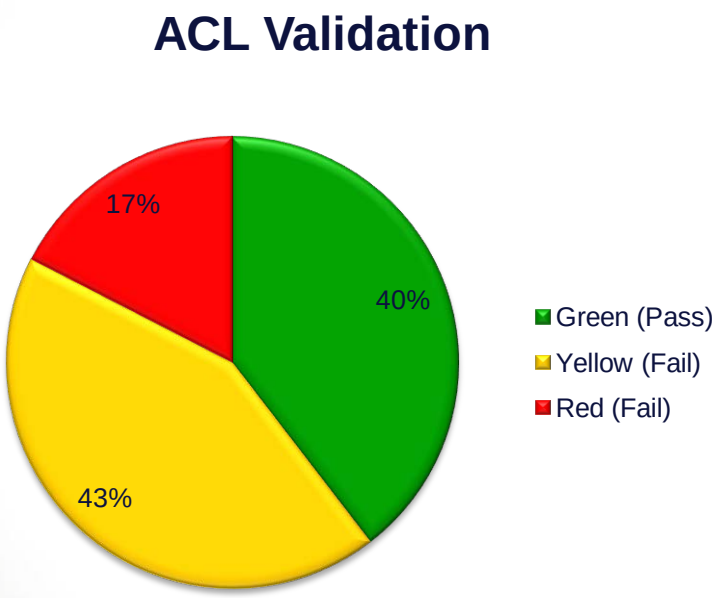


- It took approximately 7 months to isolate the medical devices behind VLANs to meet MDIA guidance

…MDPP is Now in an Operations and Maintenance (O&M) Phase…

VA INFORMATION PROTECTION

MDPP is Currently Focused on the Validation Phase of the O&M Process



**** 86 ACLs at 6 Facilities were reviewed***

Validation

- VA's IT personnel are reviewing all ACLs
- VA has begun validation assessments of the program as of FY11 Q2, ensuring that the VLANs are in place and maintained
- Multiple compliance and oversight audits occur independently of one another

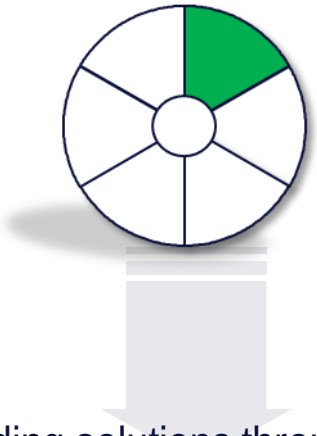
VA INFORMATION PROTECTION

Table of Contents

VA INFORMATION PROTECTION

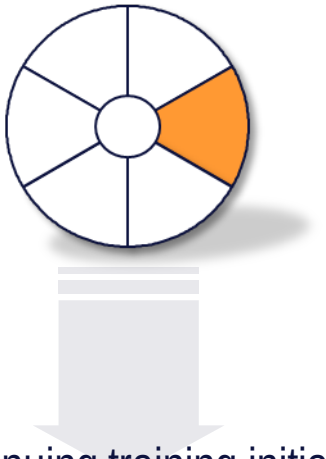
VA is Moving Forward with Numerous MDPP Activities

Communications:



- Building solutions through collaboration to reduce risk and promote innovation in the medical device network
- Working with internal and external partners to identify leading information protection and security best practices

Training:

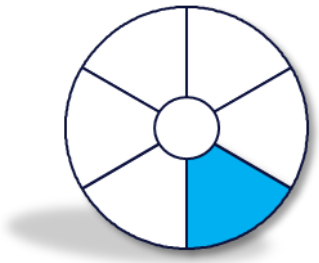


- Continuing training initiatives
  - Closing out Medical Device Incident Response (MDIR) training
  - Presenting MDPP to all VA regional facilities
  - Conducting targeted trainings at VA facilities requesting additional support

VA INFORMATION PROTECTION

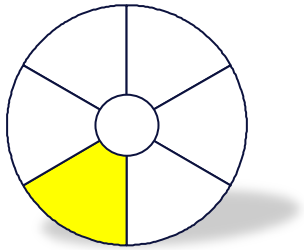
VA is Moving Forward with Numerous MDPP Activities …(con't)

Validation:



- Employing validation assessments to maintain the integrity of the MDIA implementation
  - Internal validation process began 2nd Qtr FY11
- Working on Medical Device Sanitization Guidance

Scanning:

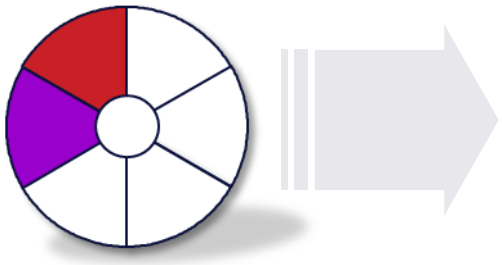


- Planning a pilot program to formalize operating procedures for scanning medical devices
- Continuing regularly scheduled scans in conjunction with local facility Biomedical Engineering
- Scanning devices upon initial introduction to network
- Tracking vulnerabilities to risk posture

VA INFORMATION PROTECTION

VA is Moving Forward with Numerous MDPP Activities…(con't)

Remediation/Patching :

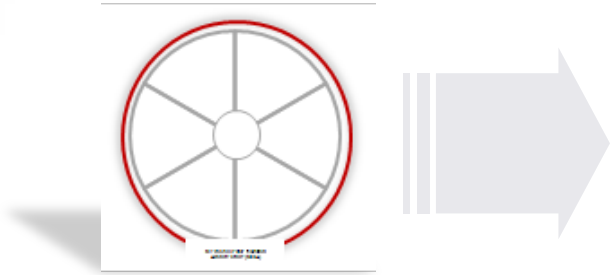


- Looking to IT staff, Biomedical Engineering, and device manufacturers to resolve problems
- Developing technical solutions and providing oversight of device manufacturers
- Relying on user facilities to keep FDA informed of device malfunctions
- Activating a single patching server for all medical devices to use
- Initiating a pilot test of a vendor patching solution
  - Installation of the hardware and software underway

VA INFORMATION PROTECTION

VA is Moving Forward with Numerous MDPP Activities…(con't)

MDIA:



- Developing strategy and technology for tighter security boundary, audit capabilities, and threat detection
- Refreshing 2009 MDIA Guidance
- Rewriting the ACL Rule set
- Drafting MDPP Security Architecture Requirements document

VA INFORMATION PROTECTION

Table of Contents

VA INFORMATION PROTECTION

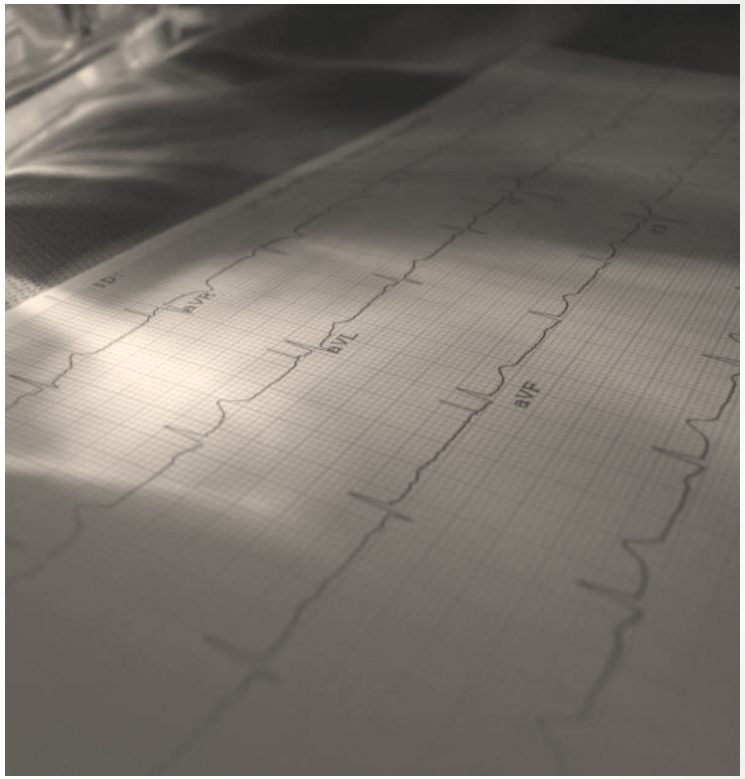
MDPP is Only as Good as the Sum of Its Parts

…Success depends on *teamwork*, *communication*, and *compliance* with established protocols

VA INFORMATION PROTECTION

Wrap Up: Medical Device Security Best Practices

- Requires an organization approach
- Needs to become a core competency of the Biomedical Engineering community
- Will have many partners, but we need to own the security of our devices
- Must have a thoughtful, well reasoned, risk based approach that recognizes that medical devices, at times, need to be treated differently



...VA is committed to ensuring the security of medical devices and upholding the world class patient care that our Nation's Veterans expect from us

VA INFORMATION PROTECTION

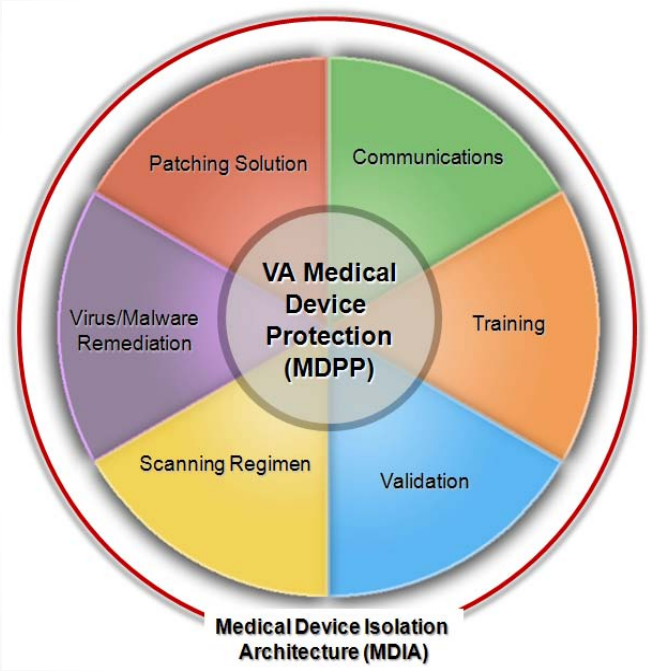
Wrap Up: MDPP Requirements

- Pre-procurement assessments must be complete
- No Internet access
- Always scan media
- No changes to ACLs without Change Control Board (CCB) approvals
- Use the Patch Repository
- Update DAT files often

…These are requisites for good computing and can be applied beyond medical device security

VA INFORMATION PROTECTION

Questions?



VA Key Contacts

Field Security Services (FSS) Health Information Security Division (HISD): VAFSOHISD@va.gov

Veterans Health Administration (VHA) Healthcare Technology Management (HTM): VHACOHTMIT@va.gov

VA INFORMATION PROTECTION