VA
Medical Device Protection Program

presented to

Information Security and Privacy Advisory Board

March 4, 2011

Table of Contents

Achieving security takes teamwork…

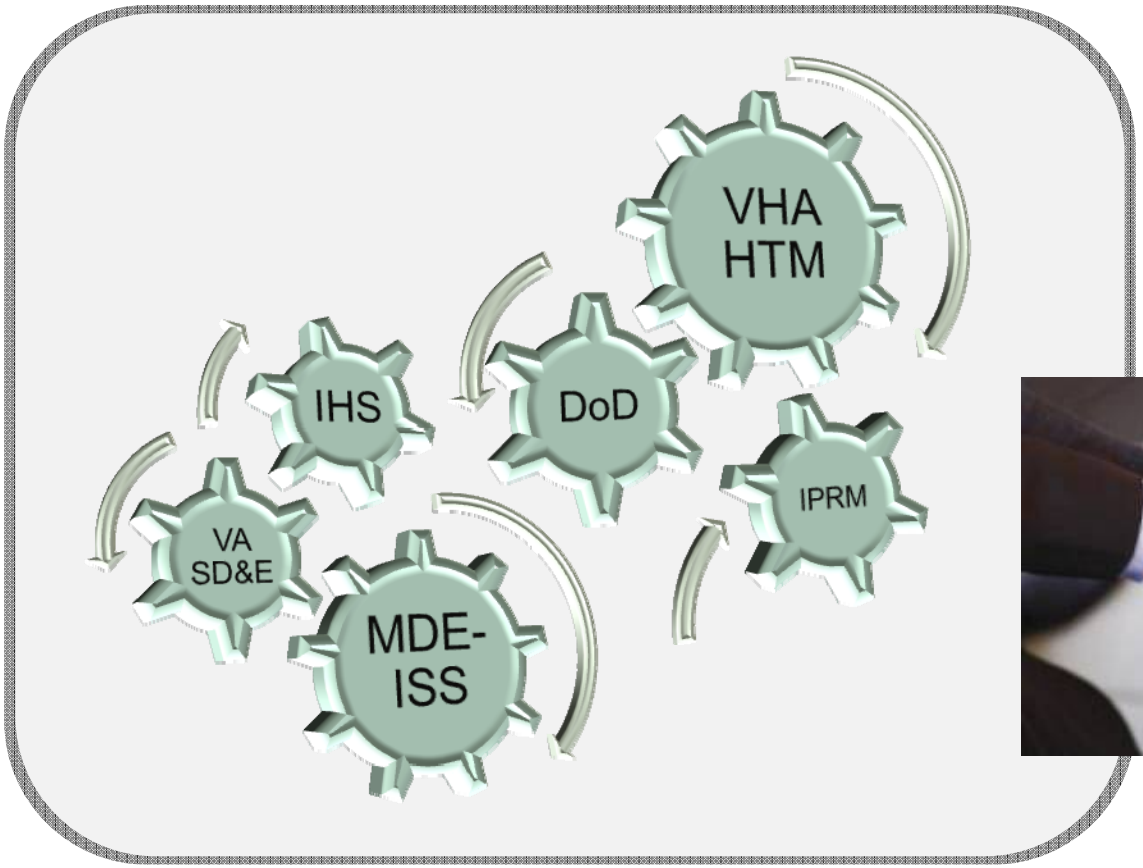


Photo Source: Idaho Department of Commerce

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!

Threats to VA Medical Devices

- **Medical devices can restrict the application of operating system patches and malware protection updates. This 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:

- 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

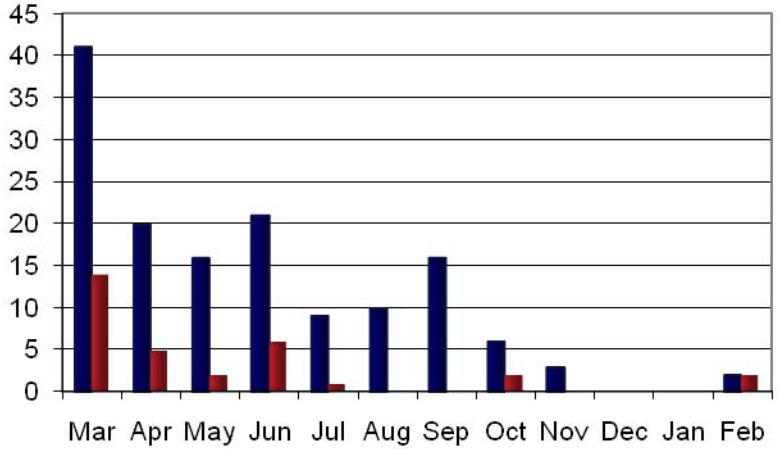
Networked medical device: Any medical device that is connected to the VA network.

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.

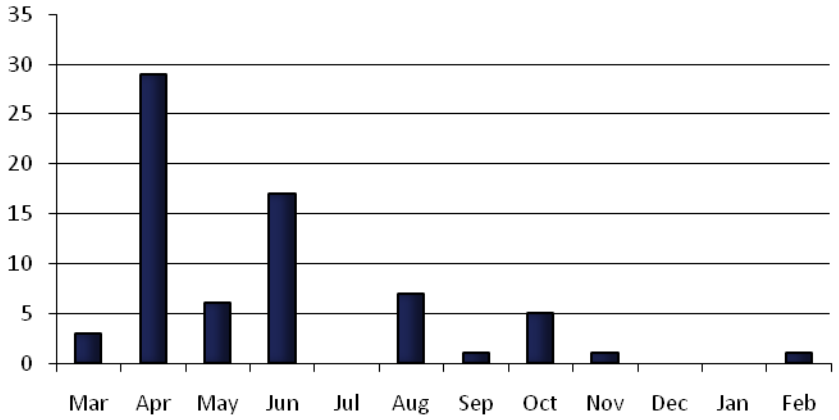
Threats to VA Medical Devices…(con't)

- **The VA-NSOC is tracking reported incidents on networked devices.**

USB Device Incidents and Infections
Mar 2010 – Feb 2011 *



Medical Device Infections
Mar 2010 – Feb 2011

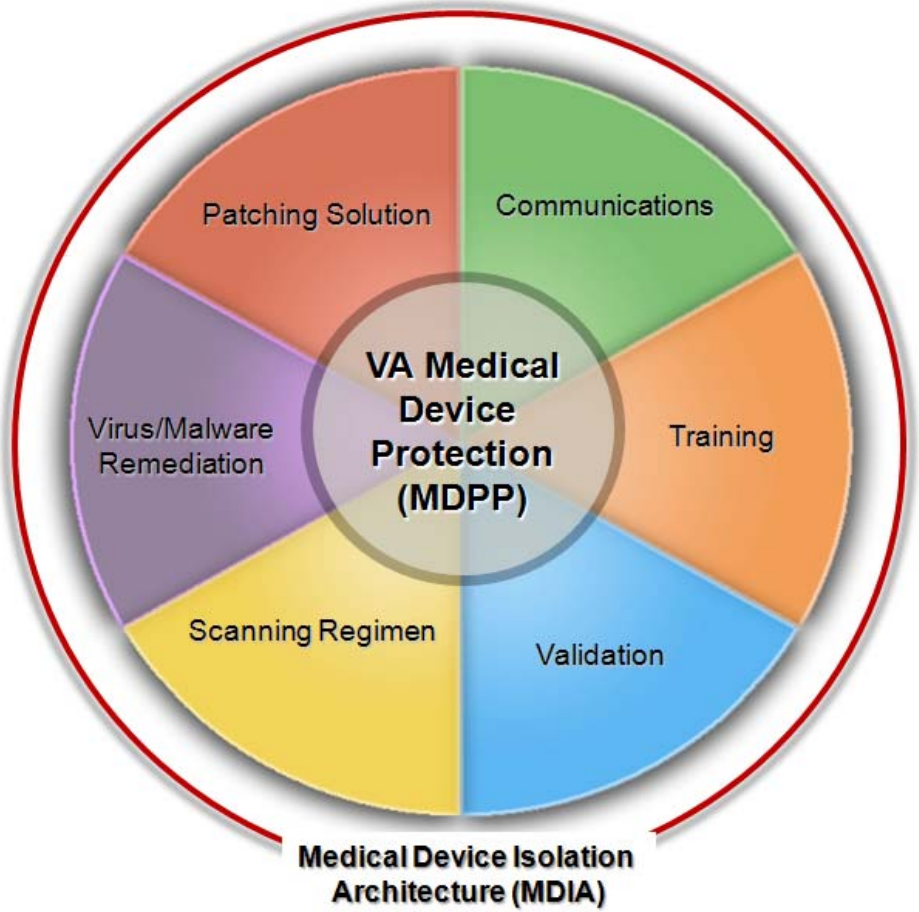


(Source: VA-NSOC Weekly Threat Briefs) * *30% of unauthorized USB incidents result in malware infection*

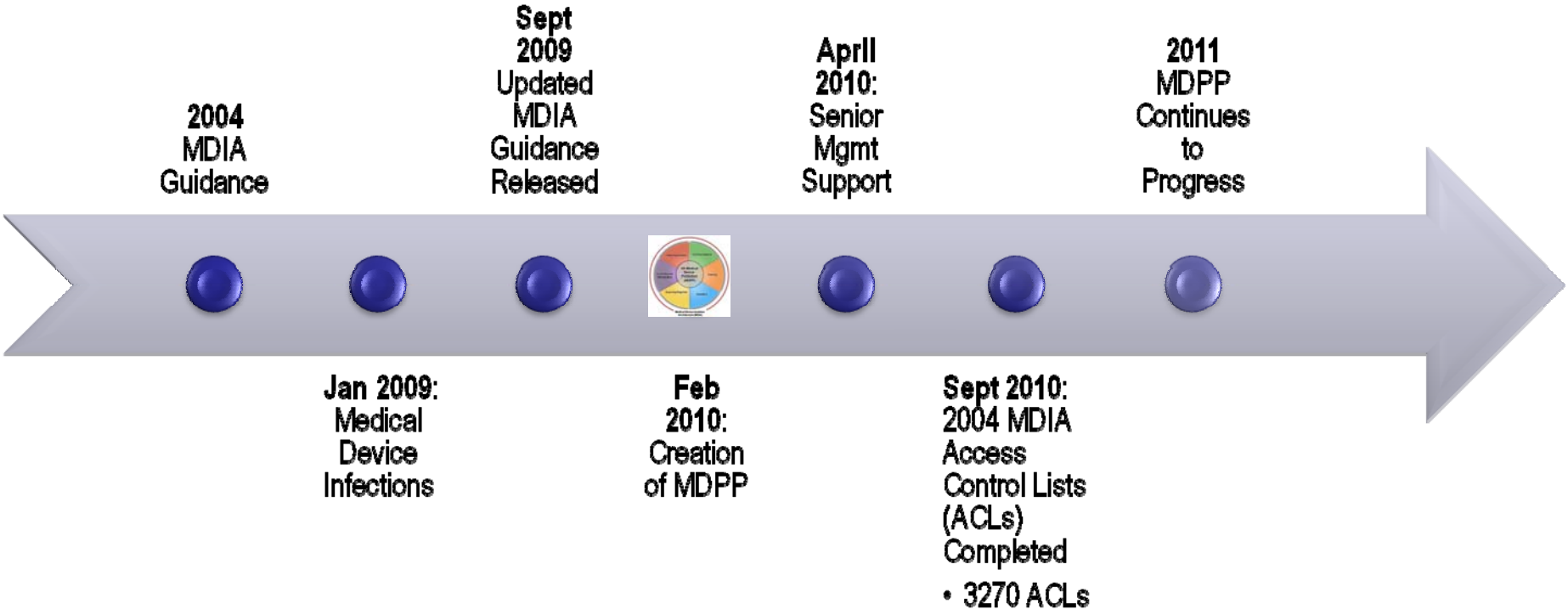
Table of Contents

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)**



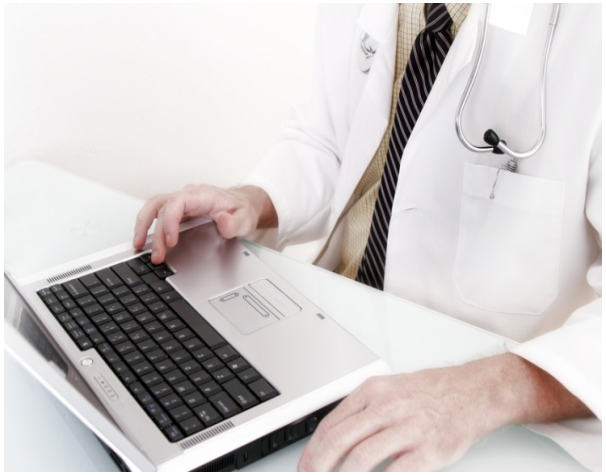
MDPP has evolved over time…



- **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**

MDIA has been implemented VA-wide

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



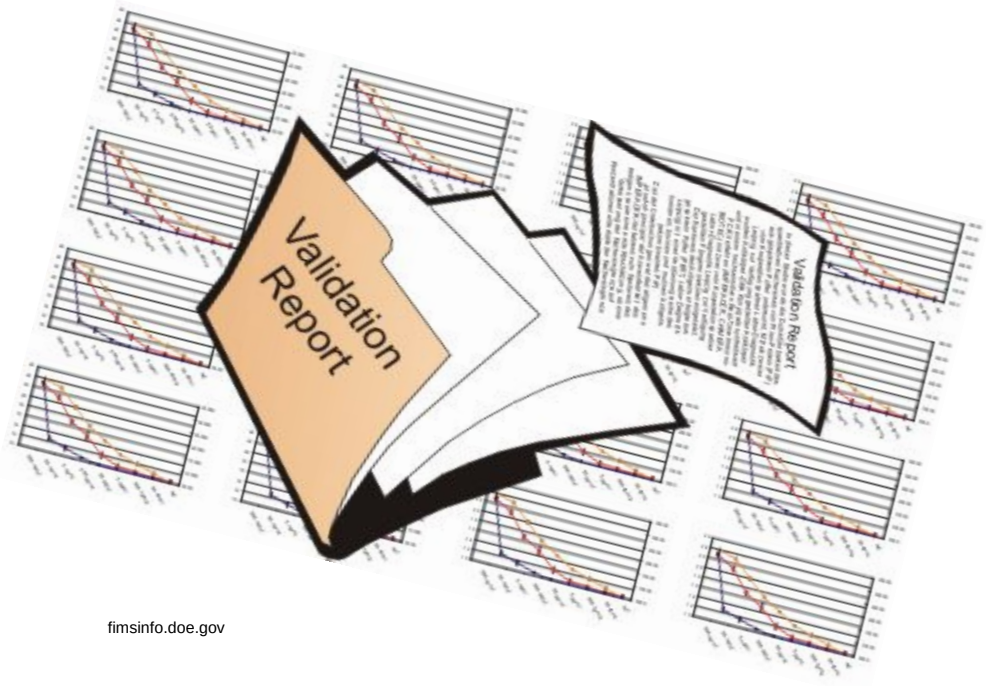
- It took approximately 7 months to isolate the medical devices behind VLANs to meet MDIA guidance

MDPP is now in an operation and maintenance (O&M) phase…

MDPP is currently focused on the validation phase of the O&M process…

Validation

- The Office of Information and Technology (OI&T) is reviewing all ACLs that have been put in place
- The Office of IT Oversight & Compliance (ITOC) and Office of Inspector General (OIG) will begin validation assessments of the program in FY11 Q2, ensuring that the VLANs are in place and maintained
- ITOC and OI&T compliance and oversight audits occur independently of one another



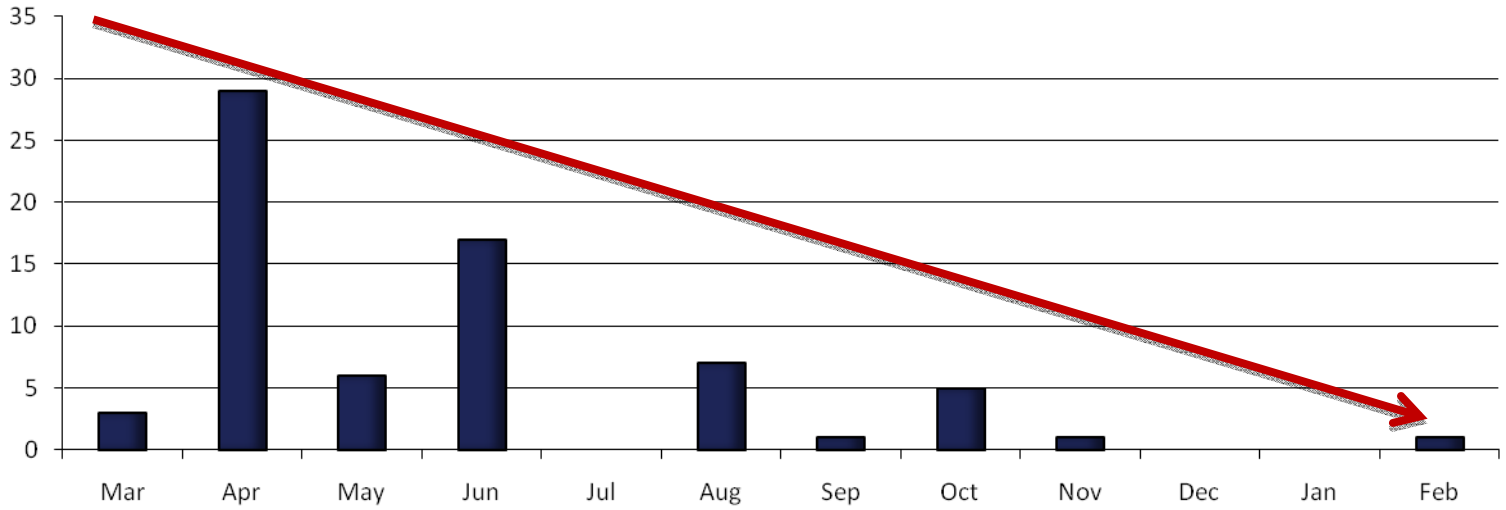
fimsinfo.doe.gov

Photo fimsinfo.doe.gov

MDPP Progress: Where are we now, and where are we going?

- **Over the time period of ACL implementations the infection rate has trended down**

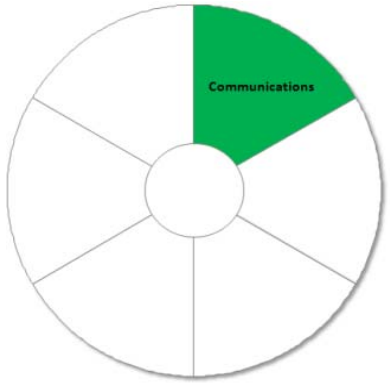
Medical Device Infections Trending
Mar 2010 – Feb 2011



Source: VA-NSOC Weekly Threat Briefs

Table of Contents

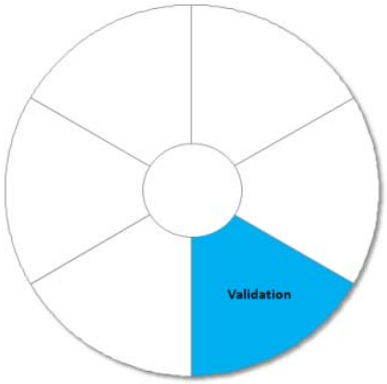
VA is moving forward with numerous MDPP activities



- **Building solutions through collaboration to reduce risk and promote innovation in the U.S biomedical device network**
  - **Participating in the launch and development of the Medical Device and Electronic Health Record Innovation, Safety and Security Consortium (MDEISS)**

- **Continuing training initiatives**
  - **MDPP Incident Response training scheduled March 2011**
  - **Presenting MDPP at all ISO & CIO regional meetings and orientations**

MDPP activities…(con't)

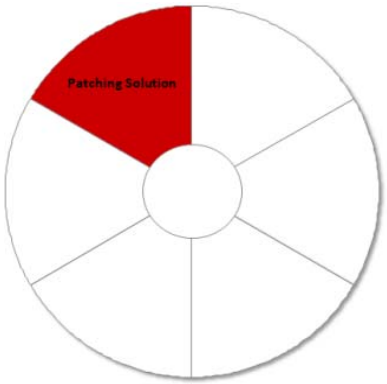


- **Employing OIG and ITOC assessments to maintain the integrity of the MDIA implementation**
  - **ITOC Validation begins 2nd Qtr FY11**
- **Publishing Medical Device Sanitization Guidance developed jointly with OI&T and VHA HTM**
  - **Scheduled for release 2nd Qtr FY11**

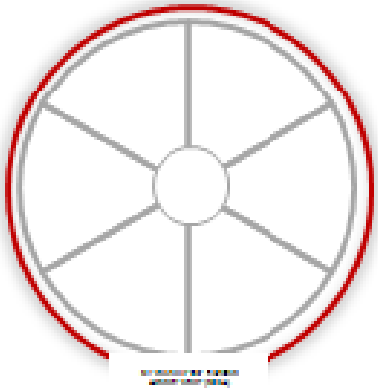
- **Working with FDA on medical device security***
  - **Looking to IT staff, biomedical engineers, and medical device manufacturers to resolve problems**
  - **Helping to develop technical solutions and providing oversight to ensure medical device manufacturers are doing their fair share**
  - **Relying on user facilities to keep FDA informed of medical device malfunctions**

** FDA has stated no legal restriction on patching of medical devices or anti-virus updates except that they must be tested by the vendor prior to VA implementation*

MDPP activities…(con't)



- **VHA Biomedical Engineer is leading a pilot test of a vendor patching solution.**
  - **This solution is limited by Vendor and Device**



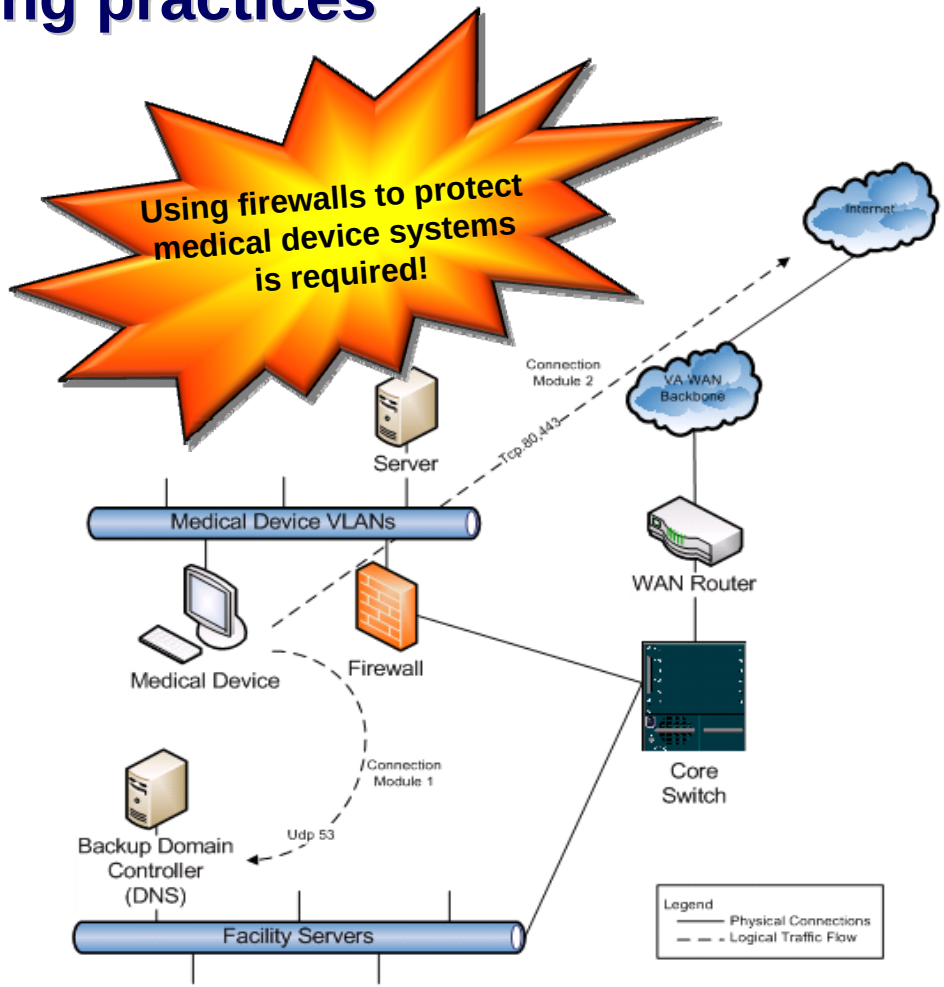
- **Developing a strategy for the deployment of firewalls to medical device VLANs for tighter security boundary and audit capabilities (MDIA)**

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

Firewalls provide packet inspection, audit capability and are hardened against attacks directed at them

Inbound firewall rule sets are applied to each 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)

Table of Contents

MDPP is only as good as the sum of its parts

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

Wrap Up: MDPP Best Practices

Hard outer shell….

Soft in the middle…..

- **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**

Author Geoff Lane/Wikimedia Commons

These are best practices for good computing and can be applied beyond medical device security!

Questions?

MDPP guidance documents can be found on the HISD portal:

https://vaww.infoprotection.va.gov/fieldsecurity/HISD.aspx

Field Security Services
Health Information Security Division
vafsohisd@va.gov