

2016 Defense Health Information Technology Symposium

Cybersecurity Aspects of Medical Device Integration



“Medically Ready Force...Ready Medical Force”

Learning Objectives

- Describe the security challenges presented by connected medical devices
- List examples of how compromised medical device data can have a major impact on patient safety
- Estimate the number of medical devices present in MHS Medical Treatment Facilities that are potentially vulnerable to data compromise using typical industry benchmarks
- Describe why data on medical devices can be more vulnerable and much more difficult to secure than data found on most IT equipment and why traditional vulnerability assessment tools may not be adequate
- Describe current MHS governance initiatives designed to address medical device security issues on an enterprise basis
- Describe current government medical device research and security initiatives and the future landscape for medical device cybersecurity

Agenda

- Mission and organization
- Cybersecurity aspects of integrated medical devices

Program Executive Office Defense Healthcare Management Systems (DHMS)

Mission and Organization



“Medically Ready Force...Ready Medical Force”

Program Executive Office Defense Healthcare Management Systems Mission



Defense Health Agency

2016 Defense Health Information Technology Symposium

To efficiently improve healthcare for the active duty military, Veterans, and beneficiaries by:

- Establishing seamless medical data sharing between DoD, the VA, and the private sector
- Modernizing the electronic health record (EHR) for the Military Health System



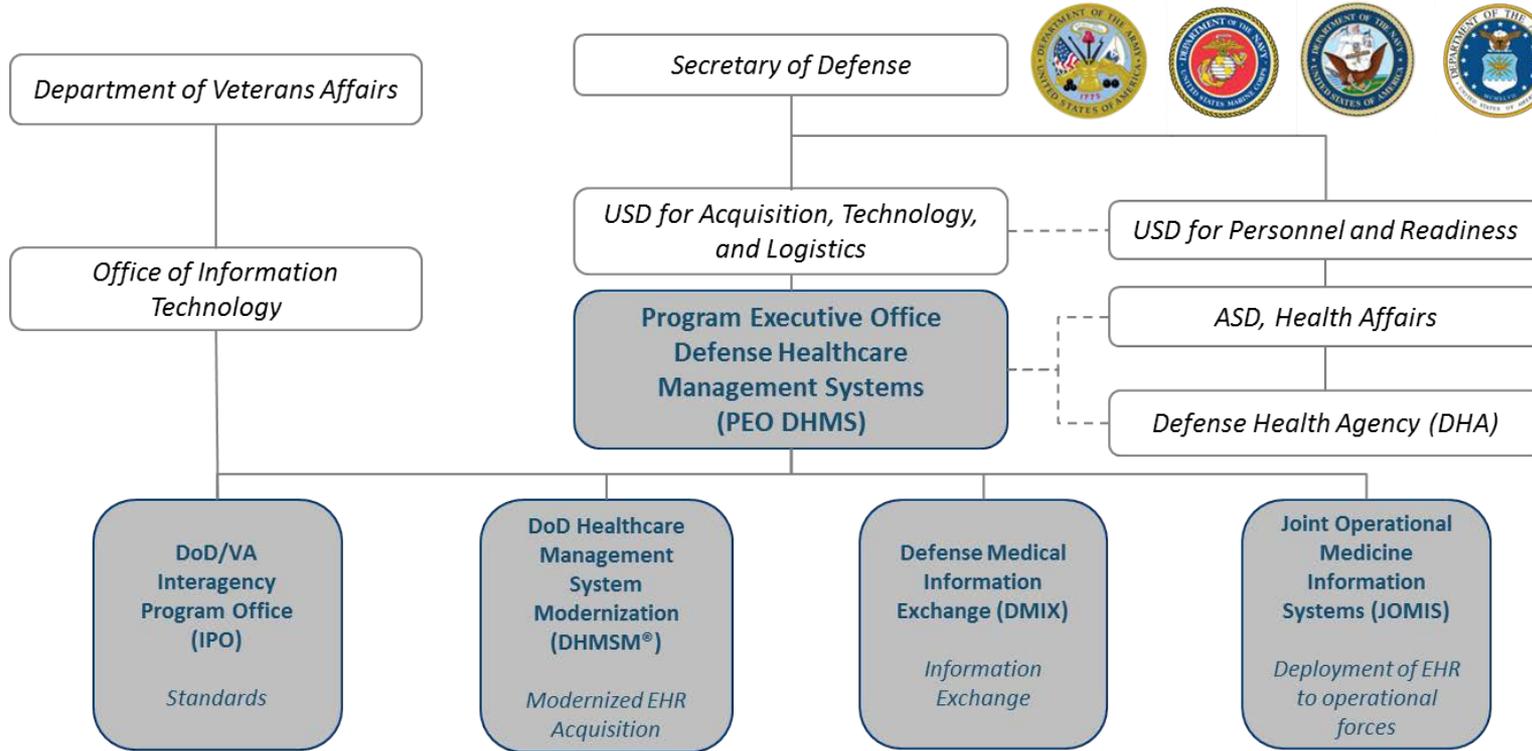
“Medically Ready Force...Ready Medical Force”

PEO DHMS Alignment



Defense Health Agency

2016 Defense Health Information Technology Symposium



“Medically Ready Force...Ready Medical Force”

DHMSM PMO Mission

Mission

The mission of the DoD Healthcare Management System Modernization (DHMSM®) Program Management Office (PMO) is to test, deliver, integrate, and successfully transition to a state-of-the-market electronic health record (EHR).

Key Objectives

INTEROPERABILITY with the standardized healthcare data framework and exchange standards

ALIGNMENT with Office of the National Coordinator standards

OPEN ARCHITECTURE for platform flexibility

SCALABILITY based on virtualization and horizontally scalable system architecture

DATA CENTRICITY between DoD, VA, and private industry

ACCOMMODATE the nuances of en route care

“Medically Ready Force...Ready Medical Force”

Program Executive Office Defense Healthcare Management Systems

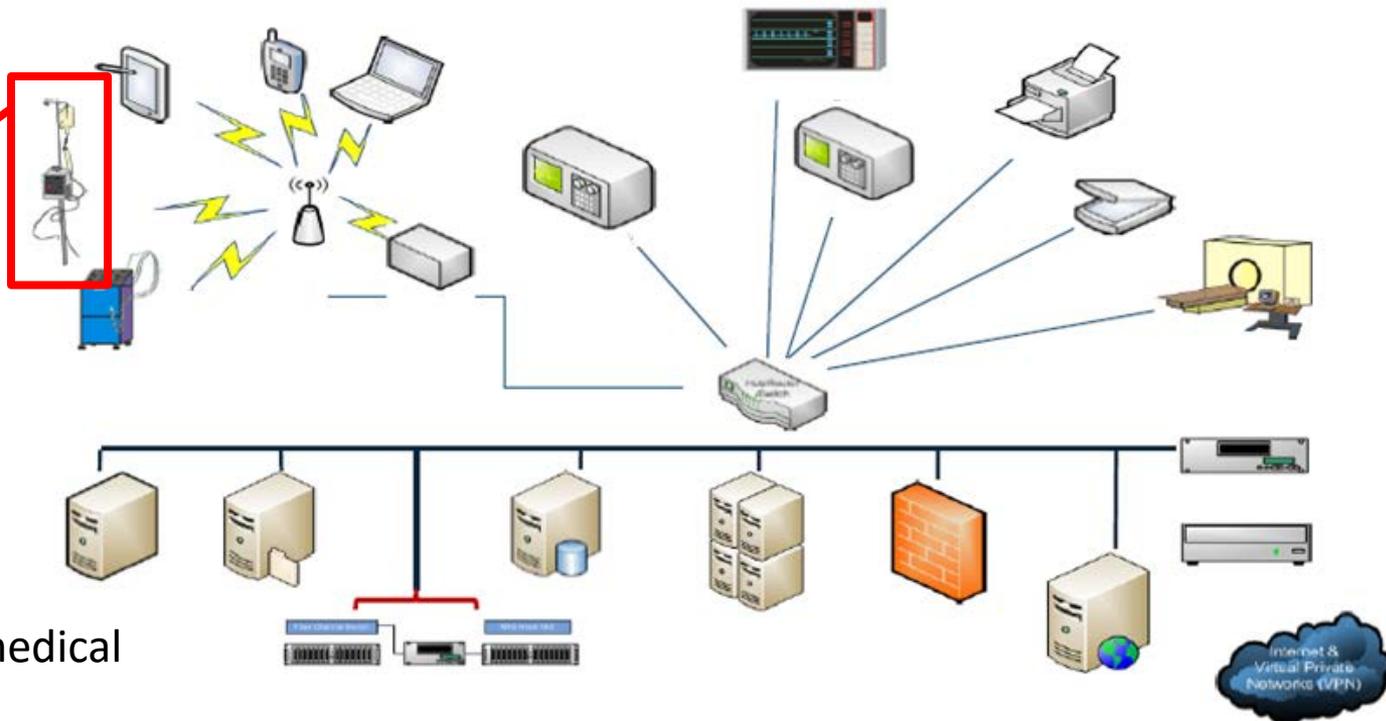
Cybersecurity Aspects of Integrated Medical Devices



“Medically Ready Force...Ready Medical Force”

- Medical Devices:
 - Exponential growth of connected hardware (LAN/WIFI)
 - Rely upon computers, software, and networking
 - May also incorporate third-party software
 - Subject to regulation, which can impact patching and reconfiguration
 - Undergo limited clinical trials
 - Often developed without secure development techniques

Typical Hospital Network – System of Systems (SoS)



SoS integrate:

- ✓ Medical & non-medical
- ✓ New & legacy

“Medically Ready Force...Ready Medical Force”

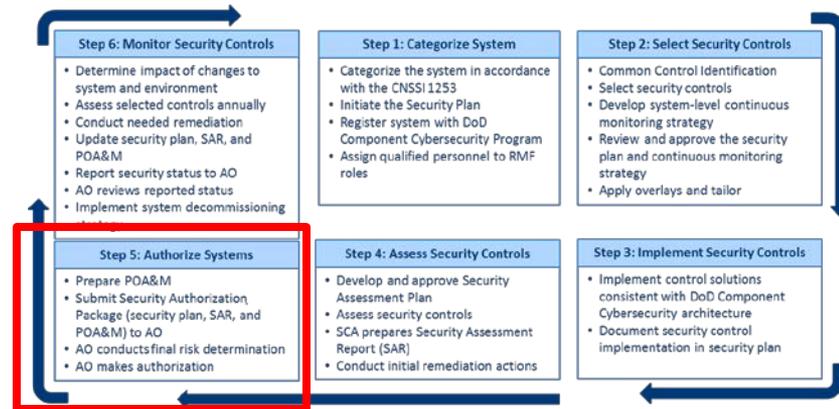
Hospira LifeCare Patient Controlled Anesthesia Vulnerabilities

- Hackers can upload medication library from unauthorized source
- Attack surface:
 - (1) Communications module used to update Drug/Dose Library
 - (2) Serial connection to module for remote update of Library with no authentication or digital signature
 - (3) Hackers use same remote access vulnerability in updating Library

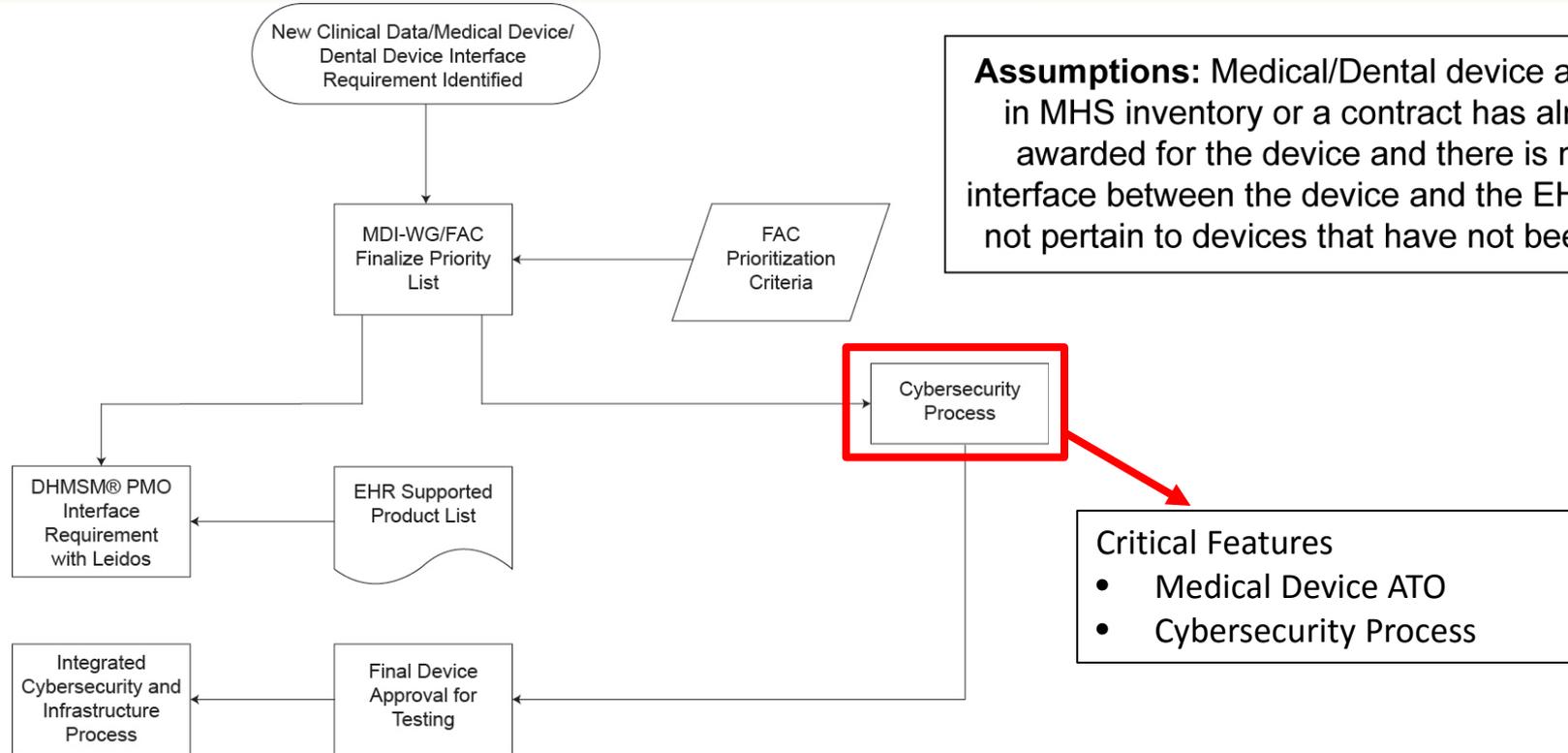


DoD Risk Management Framework (RMF)

- Step 1: Categorize system
- Step 2: Select security controls
- Step 3: Implement security controls
- Step 4: Assess security controls
- Step 5: Authorize systems
- Step 6: Monitor security controls



Proposed DHA Medical Device Acceptance Process



Assumptions: Medical/Dental device already exists in MHS inventory or a contract has already been awarded for the device and there is no existing interface between the device and the EHR. This does not pertain to devices that have not been procured.

Key Takeaways

- Connected medical devices are growing at exponential rates in healthcare
- Significant cultural and process gaps still exist
- Traditional data security measures are often not safe or appropriate for use on medical devices
- Healthcare organizations must be proactive and begin addressing medical device security

Questions?

Learn more:

-  www.health.mil/dhms
-  www.milsuite.mil/book/groups/mhs-genesis
-  @DoD_EHR
-  Defense Healthcare Management Systems

Evaluations



Defense Health Agency

2016 Defense Health Information Technology Symposium

- Please complete your evaluations

Contact Information



2016 Defense Health Information Technology Symposium

- CDR Michael Feeser
- Director of Clinical Informatics – DHMSM PMO
- dha.ncr.peo-ipo.mbx.dhmsm@mail.mil