USE CASE | HEALTH IT

FINAL DRAFT

WIRELESS MEDICAL INFUSION PUMPS

Medical Device Security

Gavin O'Brien
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

FINAL DRAFT
December, 2015
hit_nccoe@nist.gov

1. Description

Purpose

In the past, medical devices were stand-alone instruments that interacted only with the patient. Today, medical devices have operating systems and communication hardware that allow them to connect to networks and other devices. While this technology has created more powerful tools and improved health care, it has led to additional safety and security risks.

The goal of this use case is to help health care providers secure their medical devices on an enterprise network, with a specific focus on wireless infusion pumps.[1] This use case begins the process to identify the actors interacting with infusion pumps, define the interactions between the actors and the system, perform a risk assessment, identify mitigating security technologies, and provide an example implementation.

Clinicians and patients rely on infusion pumps for safe and accurate administration of fluids and medications. However, the Food and Drug Administration (FDA) has identified problems that can compromise the safe use of external infusion pumps. These issues can lead to over- or under-infusion, missed treatments, or delayed therapy.

The publication of this use case is merely the beginning of a process that will identify research participants and components of a laboratory environment to identify, evaluate, and test relevant security tools and controls. The approach may include risk assessment and analysis, logical design, build development, test and evaluation, and security control mapping. The output of the process will be the publication of a multi-part practice guide that will help the community evaluate the security environment surrounding infusion pumps deployed in a clinical setting and provide a reference solution to mitigating security tasks.

[1] The Food and Drug Administration has defined external infusion pumps as:

> "Medical devices that deliver fluids, including nutrients and medications such as antibiotics, chemotherapy drugs, and pain relievers, into a patient's body in controlled amounts. Many types of pumps, including large volume, patient-controlled analgesia, elastomeric, syringe, enteral, and insulin pumps, are used worldwide in health care facilities such as hospitals, and in the home."

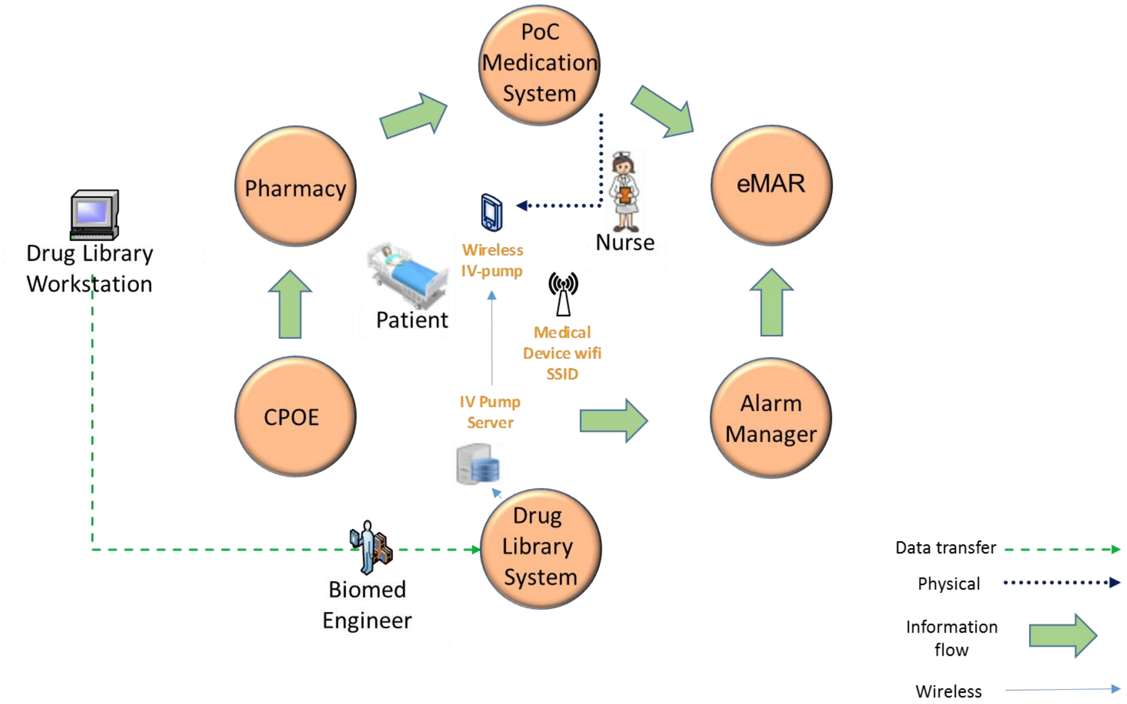
Scope

The scope of this use case is to follow the life cycle of an infusion pump from planning the purchase of the pump to decommissioning it. Life cycle management includes:

- Procurement
- Onboarding of asset
- Training and instructions for use
- Configuration
- Use
- Maintenance
- Decontamination
- Decommissioning

2. High-Level Architecture

This diagram identifies high-level areas in a hospital's technology infrastructure that may interact directly or indirectly with the patient's infusion pump. During the development of the laboratory environment implementing the use case, the diagram will be refined into component flows and mapped to a physical architecture in the lab environment.



This architecture may include:

- Patient
- Health care professional
- Wireless infusion pump
- Pump server
- Wireless network
- Alarm manager
- Electronic medication administration record (eMAR) system
- Point of care medication system
- Pharmacy
- Computerized physician order entry (CPOE)
- Drug library
- Biomedical engineering

3. Scenario

Actors

The infusion pump use case has multiple actors who may interact with the device. They interact with the relevant systems to deliver patient care in the environment. However, the environment can include bad actors. The actors include:

- Patient
- Health care professional
- Pharmacist
- Pump vendor engineer
- Biomedical engineer
- Medical information technology (IT)-network risk manager
- IT security engineer
- IT network engineer
- Central supply worker
- Patient visitor
- Hacker

Scenarios

The scenario is based on the actors and the interactions each has with an infusion pump. The scenario may be modified based upon input from the build team.

The basic scenario begins with an IT network engineer provisioning the wireless network and a biomedical engineer acquiring and connecting the infusion pump to the network. A health care professional then configures the device for use with a patient. A doctor prescribes medications for a patient and a pharmacist dispenses them. Once the device is set up and configured, a health care professional uses it on a patient. Supporting activity is provided by an IT security engineer and central supply workers, who make sure the pump is available and secure. Patient visitors may indirectly interact with health care workers if they or the patient have questions or concerns. Hackers may attempt to attack the pump through various vectors, including the pump, pump server, wireless network, clinical systems, and the hospital IT systems. Further activities include general maintenance and ultimately decommissioning and disposal of the device.

4. Current Infusion Pump Challenges

The following challenge areas will be addressed during the laboratory research and documented in the practice guide. Other challenge areas may be identified during the project.

- Access codes
- Access point (AP)/wireless network configuration
- Alarms
- Asset management and monitoring
- Authentication and credentialing
- Maintenance and updates
- Pump variability
- Use
- Emergency use

5. Business Value

This use case will provide business value to health care organizations using wireless infusion pumps. It will also provide business value to infusion pump vendors as a reference solution to vulnerabilities is identified. Additional value includes:

- Reduced errors
- Provide secured medical devices that balance usability and protection of the information and data with protection of the network
- Provide medical devices that balance security features with patient safety
- Reduce total outlays in redundant enterprise network security systems by improving security of medical devices

- Broaden visibility of user behavior in accessing and working on enterprise health care networks in order to bolster identity and access management capabilities
- Reduce the negative impacts to the reputation of the institution
- Assist in educating high-level management on the impact to the institution
- Reduce development time and increase adoptability for manufacturers

6. Requirements

1. Medical devices and associated systems
   - Wireless infusion pump
   - Pump server
   - Pump server must be capable of interfacing with at least one of the wireless infusion pumps used in the build.

     Related standards:

     - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098
2. Network
   - Enterprise-grade wireless APs with extended service set capability

     Related standards:

     - FDA, Radio Frequency Wireless Technology in Medical Devices – Guidance for Industry and Food and Drug Administration Staff, Document issued on August 12, 2013 http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf
     - NIST SP 800-48 Rev 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf
     - NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
     - IEEE 802.1x, Port Based Network Access Control http://www.ieee802.org/1/pages/802.1x.html
     - IEEE 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications http://www.ieee802.org/11/

- Virtual private networks (VPNs)

  Related standards:

  - NIST SP 800-114, User’s Guide to Securing External Devices for Telework and Remote Access
    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
  - NIST SP 800-46 Rev 1, Guide to Enterprise Telework and Remote Access Security
    http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf
  - NIST SP 800-77, Guide to IPsec VPNs
    http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf
  - NIST SP 800-52 Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

- Enterprise-grade network components, such as switches/routers

  Related standards:

  - IEEE 802.1x, Port Based Network Access Control
    http://www.ieee802.org/1/pages/802.1x.html
  - IEEE 802.3, IEEE Standard for Ethernet
    http://www.ieee802.org/3/
  - IEEE 802.1Q, Bridges and Bridged Networks
    http://www.ieee802.org/1/pages/802.1Q.html
  - Internet Engineering Task Force (IETF) Request for Comments (RFC) 4301, Security Architecture for the Internet Protocol
    https://tools.ietf.org/html/rfc4301

- Firewalls

  Related standards:

  - NIST SP 800-41 Rev 1, Guidelines on Firewalls and Firewall Policy
    http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

- Application gateways

  Related standards:

  - NIST SP 800-95, Guide to Secure Web Services
    http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

- Intrusion detection and prevention systems

  Related standards:

  - NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

3. IT systems

- Encryption tools

  Related standards:

  - NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf
  - NIST Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules http://csrc.nist.gov/groups/STM/cmvp/standards.html
  - NIST FIPS 197, Advanced Encryption Standard (AES) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

- Patch, password, and configuration management

  Related standards:

  - NIST SP 800-118, Guide to Enterprise Password Management (Draft) http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
  - NIST SP 800-40 Rev 3, Guide to Enterprise Patch Management Technologies http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
  - NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- Identity management, access control, and credentialing

  Related standards:

  - NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
  - NIST SP 800-57 Part 1 – Rev 3, Recommendation for Key Management: Part 1: General (Revision 3) http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

    - NIST SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
    - NIST SP 800-57 Part 3 Rev 1, Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

- Asset/risk management and monitoring systems

  Related standards:

    - NIST SP 800-30, Guide for Conducting Risk Assessments http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
    - NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
    - NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
    - American National Standards Institute (ANSI)/Association for the Advancement of Medical Instrumentation (AAMI)/International Electrotechnical Commission (IEC) 80001-1:2010, Application of risk management for IT Networks incorporating medical devices – Part 1: Roles, responsibilities and activities
    - IEC Technical Report (TR) 80001-2-1, Edition 1.0 2012-07, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples
    - IEC TR 80001-2-2, Edition 1.0 2012-07, TECHNICAL REPORT, Application of risk management for IT Networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
    - IEC TR 80001-2-3, Edition 1.0 2012-07, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks

  - IEC TR 80001-2-4, Edition 1.0 2012-11, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations
  - IEC TR 80001-2-5, Edition 1.0 2014-12, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems

7. Security Control Map

This table begins to map the security characteristics of the products that the NCCoE will apply to this cybersecurity challenge. It utilizes the Framework for Improving Critical Infrastructure Cybersecurity (CSF), other NIST activities, and sector-specific standards such as HIPAA. This initial mapping is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet requirements for regulatory approval or accreditation.

Example Characteristic (Based on IEC TR 80001-2-2)		Cybersecurity Standards & Best Practices			Sector-Specific Standards & Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	IEC TR 80001-2-2
Automatic logoff	Reduce the RISK of unauthorized access to HEALTH DATA from an unattended workspot. Prevent misuse by other users if a system or workspot is left idle for a period of time. Prevent access to device/system configuration data and settings.	PROTECT (PR)	Access Control (PR.AC)		ALOF
Audit controls	Define harmonized approach toward reliably auditing who is doing what with HEALTH DATA and device access, allowing the Healthcare Delivery Organization IT to monitor this using public frameworks, standards, and technology.	PROTECT (PR)	Data Security (PR.DS)	PR.DS-4	AUDT
			Protective Technology (PR.PT)	PR.PT-1	
		DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-2, DE.AE-3	
			Security Continuous Monitoring (DE.CM)	DE.CM-1, DE.CM-3, DE.CM-7	
			Detection Processes (DE.DP)	DE.DP-4	
		RESPOND (RS)	Communications (RS.CO)	RS.CO-2	
			Analysis (RS.AN)	RS.AN-1, RS.AN-3	
Authorization	Following the principle of data minimization and least privilege, provide control of access to HEALTH DATA and functions only as necessary to perform the tasks required by the HDO consistent with the INTENDED USE.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-1, PR.AC-4	AUTH
			Data Security (PR.DS)	PR.DS-5	
			Information Protection Processes and Procedures (PR.IP	PR.IP-3	
			Protective Technology (PR.PT)	PR.PT-3	
			Anomalies and Events (DE.AE)	DE.AE-1	
			Security Continuous Monitoring (DE.CM)	DE.CM-1, DE.CM-3	
Configuration of security features	Allow the HDO to determine how to utilize the product SECURITY CAPABILITIES to meet their needs for policy and/or workflow.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-1, PR.AC-4	CNFS
			Data Security (PR.DS)	PR.DS-5, PR.DS-7	
			Information Protection Processes and Procedures (PR.IP)	PR.IP-1, PR.IP-3	
			Protective Technology (PR.PT)	PR.PT-3	
		DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1	
			Security Continuous Monitoring (DE.CM)	DE.CM-1, DE.CM-3	
Cyber security product upgrades	Create a unified way of working. Secure installation / upgrade of product security patches by on-site service staff, remote service staff, and possibly authorized HDO staff (downloadable patches).	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-1, PR.IP-3	CSUP
		PROTECT (PR)	Maintenance (PR.MA)	PR.MA-1, PR.MA-2	

Example Characteristic (Based on IEC TR 80001-2-2)		Cybersecurity Standards & Best Practices			Sector-Specific Standards & Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	IEC TR 80001-2-2
Data backup and disaster recovery	Ensure that the health care provider can continue business after damage or destruction of data, hardware, or software.	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-5, ID.AM-6	DTBK
			Business Environment (ID.BE)	ID.BE-1, ID.BE-4, ID.BE-5	
		PROTECT (PR)	Data Security (PR.DS)	PR.DS-4	
			Information Protection Processes and Procedures (PR.IP)	PR.IP-4, PR.IP-7, PR.IP-9, PR.IP-10	
			Protective Technology (PR.PT)	PR.PT-4	
		DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5	
		RESPOND (RS)	Analysis (RS.AN)	RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4	
			Response Planning (RS.RP)	RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4	
			Improvements (RS.IM)	RS.IM-1, RS.IM-2	
			Mitigation (RS.MI)	RS.MI-1, RS.MI-2	
			Response Planning (RS.RP)	RS.RP-1	
		RECOVER (RC)	Communications (RC.CO)	RC.CO-3	
			Recovery Planning (RC.RP)	RC.RP-1	
Emergency access	Ensure that access to protected HEALTH DATA is possible in case of an emergency or disaster situation requiring immediate access to stored HEALTH DATA.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-1, PR.AC-4	EMRG
			Security Continuous Monitoring (DE.CM)	DE.CM-1, DE.CM-3	
HEALTH DATA de-identification	Ability of equipment (application software or additional tooling) to directly remove information that allows identification of PATIENT. Data scrubbing prior to shipping back to factory; architecting to allow remote service without HEALTH DATA access/exposure; in-factory quarantine, labelling, and training.	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-6, PR.IP-8	DIDT
HEALTH DATA integrity and authenticity	Ensure that HEALTH DATA has not been altered or destroyed in nonauthorized manner and is from the originator. Ensure integrity of HEALTH DATA, including protection from unauthorized remote access and remote programming.	PROTECT (PR)	Data Security (PR.DS)	PR.DS-1, PR.DS-2, PR.DS-6	IGAU
		DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-4	
			Detection Processes (DE.DP)	DE.DP-3	

Example Characteristic (Based on IEC TR 80001-2-2)		Cybersecurity Standards & Best Practices			Sector-Specific Standards & Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**IEC TR 80001-2-2**
Malware detection/protection	Product supports regulatory, HDO, and user needs in ensuring an effective and uniform support for the prevention, detection, and removal of malware. This is an essential step in a proper defense-in-depth approach to security.	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-7, PR.IP-12	MLDP
		DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4	
Node authentication	Authentication policies need to be flexible to adapt to local HDO IT policy. As necessary, use node authentication when communicating HEALTH DATA.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-3, PR.AC-4, PR.AC-5	NAUT
Person authentication	Authentication policies need to be flexible to adapt to HDO IT policy. This requirement is a logical place to require person authentication when providing access to HEALTH DATA. To control access to devices, network resources, and HEALTH DATA and to generate non-repudiatable audit trails. This feature should be able to identify unambiguously and with certainty the individual who is accessing the network, device, or resource. This feature should be consistent with emergency/disaster situations identified above.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-1, PR.AC-3, PR.AC-4	PAUT
Physical locks on device	Ensure that unauthorized access does not compromise the system or data confidentiality, integrity, and availability.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-2	PLOK
Security guides	Ensure that security guidance for OPERATORS and administrators of the system is available. Separate manuals for OPERATORS and administrators (including Medical Device Manufacturer sales and service) are desirable, as they allow understanding of full administrative functions to be kept only by administrators.	Can be mapped to multiple places as this is for OPERATORS and administrators			SGUD
System and application hardening	Adjust security controls on the MEDICAL DEVICE and/or software applications such that security is maximized ("hardened") while maintaining INTENDED USE. Minimize attack vectors and overall attack surface area via port closing; service removal, etc.	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-1, PR.IP-2	SAHD
Third-party components in product	Goal is to proactively manage impact of life cycle of components throughout a product's full life cycle. This	IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-1	RDMP
			Risk Assessment (ID.RA)	ID.RA-1	

Example Characteristic (Based on IEC TR 80001-2-2)		Cybersecurity Standards & Best Practices			Sector-Specific Standards & Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	IEC TR 80001-2-2
lifecycle roadmaps	commercial off-the-shelf or 3rd party software includes operating systems, database systems, report generators, Medical Imaging Processing components, etc. (assumption is that existing Product Creation Process already manages hardware component obsolescence). 3rd party includes here also internal suppliers of security vulnerable components with own life cycle and support programs.	PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-3	
			Maintenance (PR.MA)	PR.MA-1	
			Information Protection Processes and Procedures (PR.IP)	PR.IP-1, PR.IP-2, PR.IP-3	
		DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-6	
HEALTH DATA storage confidentiality	MDM establishes technical controls to mitigate the potential for compromise to the integrity and confidentiality of HEALTH DATA stored on products or removable media.	PROTECT (PR)	Data Security (PR.DS)	PR.DS-1, PR.DS-5	STCF
Transmission confidentiality	MANUFACTURER demonstrates that its equipment meets multiple national standards or regulations (USA HIPAA, EU 95/46/EC, HBP 517, etc.) according to HDO needs to ensure the confidentiality of transmitted HEALTH DATA.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-2	TXCF
			Data Security (PR.DS)	PR.DS-2, PR.DS-5	
Transmission integrity	System/device protects the integrity of transmitted HEALTH DATA.	PROTECT (PR)	Access Control (PR.AC)	PR.AC-2	TXIG
			Data Security (PR.DS)	PR.DS-5	
		DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-4	
			Detection Processes (DE.DP)	DE.DP-3	

APPENDIX: OTHER RELEVANT REGULATIONS, STANDARDS, AND GUIDANCE

The following is a list of standards, guidance, and directives regarding cybersecurity in the medical device and health care domain. It includes NIST and international standards and guidance on cybersecurity best practices.

Regulations

- FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014 http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

- FDA, Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf

- FDA, Infusion Pumps Total Product Life Cycle - Guidance for Industry and FDA Staff, Document issued on: December 2, 2014 http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf

Health Care / Medical Devices Specific (International Oranization for Standardization [ISO]/IEC, IHE)

- Department of Homeland Security (DHS), Attack Surface: Healthcare and Public Health Sector https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php
- Department of Health and Human Services (HHS) HIPAA Administrative Simplification Statute and Rules http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html
- Integrating the Healthcare Enterprise (IHE) Patient Care Device (PCD), Technical Framework White Paper http://www.ihe.net/Technical_Framework/upload/IHE_PCD_Medical-Equipment-Management_MEM_White-Paper_V1-0_2009-09-01.pdf
- IHE PCD, White Paper, Medical Equipment Management (MEM): Cyber Security http://www.ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05-27.pdf

- IHE PCD, White Paper, MEM: Medical Device Cyber Security – Best Practice Guide http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf
- IHE PCD, Technical Framework, Volume 1, 10 IHE PCD TF-1 Profiles http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_TF_Vol1.pdf
- IHE PCD, Technical Framework, Volume 2, IHE PCD TF-2, Transactions http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_TF_Vol2.pdf
- IHE PCD User Handbook – 2011 Edition – Published 2011-08-12 http://www.ihe.net/Technical_Framework/upload/IHE_PCD_User_Handbook_2011_Edition.pdf
- Department of Veterans Affairs (VA), Medical Device Isolation Architecture Guide 2009 http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/MedicalDeviceIsolationArchitectureGuidev2.pdf

General Cybersecurity / Risk Management (ISO/IEC, NIST)

- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure http://www.nist.gov/itl/cyberframework.cfm

- NIST SP 800-160, Systems Security Engineering, An Integrated Approach to Building Trustworthy Resilient Systems http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

- SANS 20 Critical Security Controls http://www.sans.org/critical-security-controls/