CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Specification Security Considerations for Foundational Efforts

CMI-TR-F-SEC-D01-20190311

DRAFT

Notice

This specification is the result of a cooperative effort undertaken at the direction of The Center for Medical Interoperability for the benefit of the healthcare industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by The Center in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by The Center. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

DISCLAIMER

This document is furnished on an "AS IS" basis and neither The Center nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and The Center and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

The Center reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by The Center or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from The Center, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	CMI-TR-F-SEC-D01-20190311			
Document Title:	Security Considerations for Foundational Efforts			
Revision History:	D01			
Date:	March 11, 2019			
Status:	~~Work in Progress~~	**Draft**	~~Issued~~	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~The Center/Member~~	~~The Center/ Member/ NDA Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through The Center.

Contents

Figures

Tables

1 Introduction and purpose

This technical report outlines the overall security strategy The Center for Medical Interoperability (CMI), also referred to as "The Center", is implementing to achieve secure interoperability between connected devices. This informative document provides insight to how The Center will provide a trust framework and outlines foundational factors for achieving security by design. Discussions of architecture considerations and potential security threats are presented as well. This is intended to be a living document. Future iterations of the technical report will expand on and improve upon the content. Where beneficial, gaps and future work are identified.

This document focuses on factors necessary to achieve secure interoperability, but experience has demonstrated that this also requires that devices achieve some level of basic security in implementing medical, network, and common functions. Consequently, a security by design approach must be used which focuses on achieving foundational security of networked components. Center specifications will apply these foundation elements as security principals that provide secure interface implementations. This document does not, however, strongly address human factors in systems security. This is an important area, but is also very dependent on specific care institution practices and needs. Further iterations of this document may more comprehensively address this area.

This document should benefit contributors to The Center, The Center's members, and vendors supporting The Center's members. Contributors may use the ideas here to guide implementation of technology efforts. Members may also use these ideas to organize their approach to identifying and documenting their internal requirements and for guidance on how to consider security in their technical selection processes. Vendors may be able to use the technical report to better respond to member needs and provide increasingly secure solutions.

2 Informative References

This technical report uses the following informative references. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific. For a non-specific reference, the latest version applies.

2.1 United States Government References

[PPD-21] Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience", February 12, 2013

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[EO-13636] Executive Order (EO) 13636, "Improving Critical Infrastructure CyberSecurity", February 12, 2013

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[FDA-OTS-1] "Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Devices, U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Office of Compliance, Office of Device Evaluation" , September 9, 1999

https://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf

[FDA-OTS-2] "Guidance for Industry Cybersecurity for Networked Devices Containing Off-the-Shelf (OTS) Software", January 14, 2005

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf

[FDA-CS-1] "Content of Premarket Submissions for Management of Cybersecurity in Devices, Guidance for Industry and Food and Drug Administration Staff", October 2, 2014

https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf

[FDA-LC] "Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff", December 2, 2014

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf

[FDA-510K] "Deciding When to Submit a 510 K for a software change to an existing device", August 8, 2016

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM514771.pdf

[FDA-CS-2] "Postmarket Management of Cybersecurity in Devices - Guidance for Industry and Food and Drug Administration Staff Document", December 28, 2016

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[FDA-PM] "Design Considerations and Pre-market Submission Recommendations for Interoperable Devices", January 26, 2016.

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf

[NIST-800-30] NIST SP 800-30, " Guide for Conducting Risk Assessments" , Sep 2012

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[NIST-800-37] NIST SP 800-37, Rev.1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach", February 2010

http://dx.doi.org/10.6028/NIST.SP.800-37r1

[NIST-800-38A] NIST SP 800-38A, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", December 2001

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[NIST-800-53] NIST SP 800-53, Rev. 4, "Security and Privacy Controls For Federal Information Systems and Organizations", April 2013.

http://dx.doi.org/10.6028/NIST.SP.800-53r4

[NIST-800-64] NIST SP 800-64 Rev. 2, "Security Considerations in the System Development Life Cycle", October 2008

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf

[NIST-800-61] NIST SP 800-61, Rev. 2, "Computer Security Incident Handling Guide", January, 2004

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[NIST-800-65] NIST SP 800-65, "Integrating IT Security into the Capital Planning and Investment Control Process", January 2005

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-65.pdf

[NIST-800-67] NIST SP 800-67, Rev 1, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", Jan 2012

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf

[NIST-800-77] NIST SP 800-77, “Guide to IPsec VPNs”, December 2005

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

[NIST-800-160] NIST SP 800-160, “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems”, November 2016

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

[FIPS-46-3] FIPS 46-3, “Data Encryption Standard (DES)”, October 1999

http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-140-2] FIPS 140-2, “Security Requirements for Cryptographic Modules”, May 2001

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[FIPS-180-2] FIPS 180-2, “Secure Hash Standard (SHS)”, August 2002

http://csrc.nist.gov/publications/fips/fips180-2/FIPS180-2_changenotice.pdf

[FIPS-185] FIPS 185, "Escrowed Encryption Standard”, February 1994

http://csrc.nist.gov/publications/fips/fips185/fips185.pdf

[FIPS-186-2] FIPS 186-2, “Digital Signature Standard (DSS)”, January 2000

http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf

[FIPS-197] FIPS 197, "Advanced Encryption Standard”, November 2001

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS-198] FIPS 198-1, “The Keyed-Hashed Message Authentication Code (HMAC)”, July 2008

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

[FIPS-199] FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems”, Feb 2004

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[FIPS-200] FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems", March 2006

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[IATF-TR] "Information Assurance Technical Framework (IATF)", Release 3.1, NSA IA Solutions Technical Directors, September 2002

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA606355

2.2 Industry and International References

[AAMI-TIR57] AAMI TIR57/Ed. 1, "Principles for device information security--risk management", June, 2016

Preview:
http://my.aami.org/aamiresources/previewfiles/TIR57_1607_Preview.pdf

[IEC-80001] IEC 80001-1:2010, "Application of risk management for IT-networks incorporating devices -- Part 1: Roles, responsibilities and activities", Oct, 2010

https://www.iso.org/standard/44863.html

[IEC-27005] ISO/IEC 27005:2011, " Information technology -- Security techniques -- Information security risk management", June, 2011

https://www.iso.org/standard/56742.html

[IEC-15408] ISO/IEC 15408-3:2008, "Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements", Aug, 2008

https://www.iso.org/standard/46413.html

[IEC-14971] ISO/IEC 14971:2007, "Medical devices -- Application of risk management to medical devices", Mar 2007

https://www.iso.org/standard/38193.html

[IEC-29147] ISO/IEC 29147:2014, "Information technology -- Security techniques -- Vulnerability disclosure", Feb, 2014

https://www.iso.org/standard/45170.html

[IEC-30111] ISO/IEC 30111:2013, "Information technology -- Security techniques -- Vulnerability handling processes", Nov, 2013

https://www.iso.org/standard/53231.html

[IETF-RFC2196] IETF RFC 2196, "Site Security Handbook", September 1997

https://tools.ietf.org/html/rfc2196

[IETF-ID-SCEP] IETF Internet-Draft, draft-gutmann-scep-05, "Simple Certificate Enrolment Protocol"

https://www.ietf.org/id/draft-gutmann-scep-05.txt

[IEC-62443-1] IEC TS 62443-1-1:2009 "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models", Sep 2009

https://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf

[IEC-62443-2] IEC TR 62443-2-3:2015 "Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment", Jun, 2015

https://webstore.iec.ch/publication/22811

[DT-Sec] Diabetes Technology Society, "Cybersecurity Standard for Connected Diabetes Device Security", 2016

https://www.diabetestechnology.org/dtsec-standard-final.pdf

[DT-CCD] Diabetes Technology Society, "Protection Profile for Connected Diabetes Devices", May, 2016

https://www.diabetestechnology.org/dtsec-protection-profile-final.pdf

[HN-MDS] HIMSS/NEMA, "Manufacturer Disclosure Statement for Medical Device Security", October, 2013

http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx - download

[CMI-DOC-TD] "Terms and Definitions", Center for Medical Interoperability, Mar. 2019

https://medicalinteroperability.org/specifications/D01/CMI-DOC-TD-D01-20190311.pdf

2.3 Reference Acquisition

Center for Medical Interoperability, 8 City Boulevard, Suite 203 | Nashville, TN 37209;
Phone +1-615-257-6410; http://medicalinteroperability.org/

Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org

3 Terms and Definitions

This document uses the terms specified in [CMI-DOC-TD].

4 Abbreviations and Acronyms

This document uses the following abbreviations:

CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation List
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards
IETF	Internet Engineering Task Force
ISO	Independent System Operators
JTAG	Joint Test Action Group
MAC	Media Access Control
CMI	The Center for Medical Interoperability
PA	Policy Authority
PHI	Personal Health Information
PII	Personally Identifiable Information
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure

RFC	Request for comment
RSA	Rivest, Shamir, Adelman
SPI	Serial Peripheral Interface
TWH	Trusted Wireless Health

5 Introduction

Trust is a decision to believe and rely on the identity of a device or individual. This trust decision is the foundation for all other security controls and activities. Trust in The Center's intended ecosystem will be based on a public key infrastructure (PKI) which uses private keys, public keys, and certificates that are distributed and protected such that they can be a basis for strong security. The private key and certificate PKI will be the basis for authentication and key exchange which in turn enables privacy through encryption. A unique device identifier (MAC address or similar) will be included in end-entity device certificates which binds the device's identity to its authentication status and will be used to check that a device is authorized to access the network and receive services. Attestation of certificates will be provided by chaining certificates to The Center's certificate authority.

One critical gap in this paradigm is that human to machine interactions by caregivers, system administrators, and care receivers may undermine the trust framework by inadvertently or intentionally compromising devices. Consequently, The Center's security strategies must address the overall security of networked devices holistically. This is a process and result that can be referred to as security by design. Security by design implements in a security model that distributes security functions throughout the device, and as such is part of every medical and network and device function. Implementation of every security function must, in some way, even if indirectly, rely on and chain trust as described above.

The Center has identified foundational security elements that are ultimately services that network and medical functions call as necessary. These elements have been identified and defined after deep consideration of interoperable medical connectivity architecture and threats to that architecture. This consideration has resulted in a comprehensive trust framework that implements the foundational security elements such that they achieve scalability and resiliency while assuring targeted experiences to clinicians and patients as defined in Center use cases. Foundational security elements include: identity, authentication, authorization, message integrity, privacy, non-repudiation, secure configuration, secure patient to device association, secure service discovery, and upgradeable security.

This paper presents the philosophy and corresponding approach to how The Center's specifications will address security. It briefly overviews the high level architecture, discusses threats to medical infrastructure components, and then presents a security framework. The framework is based on

pervasive reliance on root of trust delivered using public key infrastructure and implementation of multiple layers of security associations to achieve defense in depth.

6 Architecture Overview

The Center has defined a basic layered architecture comprising of devices, aggregation functions, platform, and application. The Center's current focus is specification of the device to platform interface. This is shown in Figure 1 below. The initial focus of The Center specifications is secure interoperability between Gateways and the Platform Layer. This includes specification of wireless and wired connectivity and secure transport based upon IHE PCD HL7. These specifications will be used to implement other interfaces to other elements, as well.

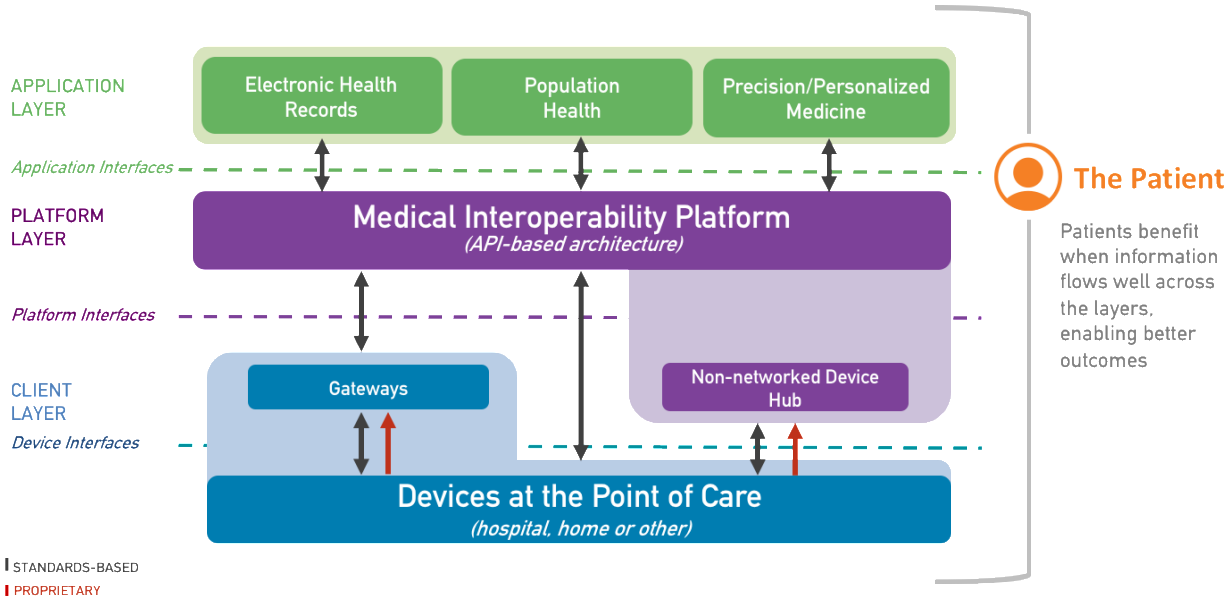

Figure 1: High-Level Architecture

6.1 Network Architecture

This architecture can also be shown in the context of a network diagram. This provides better connectivity context and is useful for understanding security requirements and considerations. One or more devices may connect to a gateway or point of care as an aggregation point. This connection may be wireless (WiFi, Bluetooth, or other) or wired (USB, Ethernet, or other). The aggregation point will be logically connected to the plug-and-and play interoperability platform and possibly management and network services (such as DNS, time servers, DHCP, configuration or boot strap servers, etc.) over the hospital network using either (or both) wireless and wired connectivity. Wireless connectivity will leverage The Center's Trusted Wireless Health (TWH) guidelines. The interoperability platform will, in turn, be logically connected to one or more medical services and also management and network services over the hospital network using either or both wireless and wired connectivity. For some ecosystem life cycle functions, connectivity to opens source and

device manufacturer services may be required which will, of course, be accomplished over the Internet or dedicated WAN connections. This architecture is shown in Figure 2.

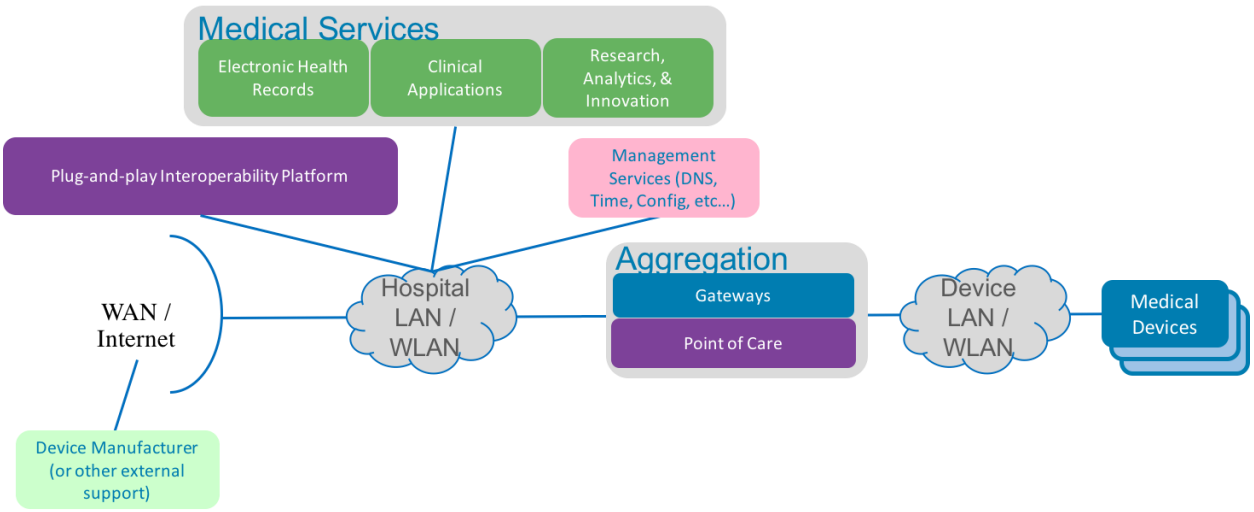

Figure 2: CMI General Network Architecture

6.2 Interfaces

Consideration of the architectures identifies many potential interfaces. These are summarized in Table 1. Interfaces that will be addressed over time are those that directly connect Devices, Gateways, Points of Care, and the Interoperability Platform. Any connectivity to these elements is strongly recommended to apply The Center's trust framework and security recommendations. Initially, The Center's initial focus will be on Gateway to Platform interoperability. Principles developed for this interface will be extended iteratively according to priorities established by The Center's members.

Table 1: Summary of Interfaces

	Device	Gateway	Point of Care	Management Services	Medical services	PnP interoperability Platform	Supply chain (vendor)
Device	✔	✔	✔	✔	✔	✔	✔
Gateway	✔	- NA -	- NA -	✔	✔	✔	✔
Point of Care	✔	- NA -	- NA -	✔	✔	✔	✔
Management services	✔	✔	✔				
Medical services	✔	✔	✔				
PnP interoperability platform	✔	✔	✔				
Supply chain (vendor)	✔	✔	✔				

7 Threat Framework and Identification

Maintaining a comprehensive threat framework is probably not within The Center's current capabilities. However, discussion of a notional framework and corresponding known threats provides context and insight useful for identifying core security requirements and needs. This section presents an overview of device security vulnerabilities, provides a reference model for discussing threats, and then provides a threat assessment.

7.1 Device Vulnerabilities

The anatomy of a connected device lends itself to traditional legacy electro-mechanical and software application design parameters that have not had cyber or information security design control considerations. Typically a device manufacturer will, under regulatory advisory from the Food & Drug Administration (FDA) conduct periodic risk and vulnerability assessments to ensure that both known and unknown vulnerabilities are discovered and architectural and design changes made to the device affected by the potential compromise.

Cyber and information security practice states fundamental objectives of device cyber security consideration as confidentiality, integrity, and availability of information. Interconnected devices are impacted in the following ways:

- Confidentiality can be compromised from unauthorized access due to inadequate or ineffective access control measures. Confidentiality impacts include, but are not limited to the following:
    - Reputational damage

- Litigation and financial consequences
- Lack of consideration for or compliance with Health and Human Services (HHS) regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Integrity of inter-networked devices may be the result of system data corruption poorly configured systems and potentially escalation of privileges resulting in unauthorized manipulation of information. Impacts to integrity are thus:
  - Threat to patient safety from device being remotely tampered with by a nefarious intruder;
  - Threat to patient safety from potentially inaccurate or incorrectly diagnosed and administered clinical decisions.
- Availability of a device during which authorized access is corrupted and or constrained thus access to data is compromised. Impacts to device availability may include the following:
  - Denial of access to authorized biomedical or clinical staff during care administration;
  - Threats to patient safety when access to relevant critical information is compromised and subsequent clinical decisions are affected;
  - Threats to patient safety when critical alerts are rendered ineffective.[1]

The confidentiality, integrity, and availability of device functions can be disrupted at the device, remotely using vulnerable communications channels, or passively by intercepting communications.

As a first step in an analysis process, the potential vulnerabilities of the device should be identified. Sources for known vulnerabilities are data published by the manufacturer or provider of the host operating system (esp. for software- only devices), publicly available vulnerability databases as well as the analysis of the device security properties identified earlier.

7.2 A Reference Network for Remote Access Threat Modeling

It is useful to be able to picture the direction of network attack to a target relative to the network in which they are deployed. A simplified architecture useful for discussing security threats is shown in Figure 3.

[1] Patricia AH Williams and Andrew J Woodward. “Cybersecurity vulnerabilities in devices: a complex environment and multifaceted problem”. 2015 Jul 20. (Internet), Accessed: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

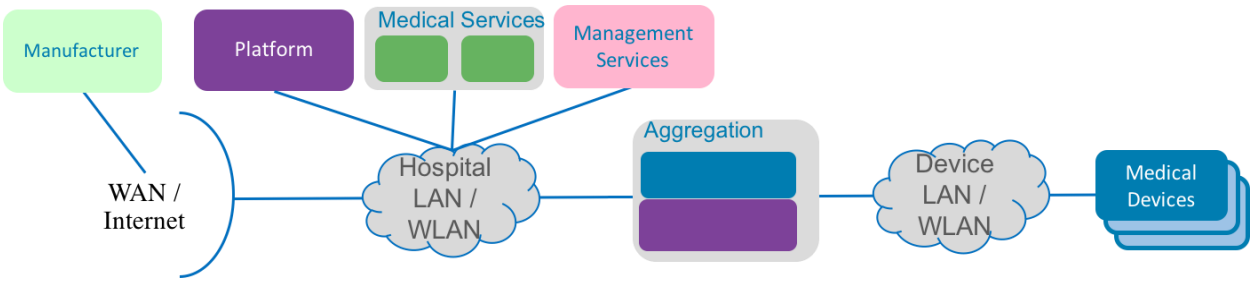

Figure 3: Reference Architecture for Threat Modeling

7.3 Threat Modeling

There are many approaches to threat modeling. Formal methods and tools are available. However, a simple approach is useful for understanding the basic landscape in which devices exist. Basic threat modeling can be performed by considering threat vectors, identifying likely common attacks, and understanding basic motivations. Given this information, mitigation strategies can be selected and tested. These ideas are briefly defined below.

- Threat vectors – ISACA defines a threat vector as "a path or tool that a threat actor uses to attack a target." The target, of course, is anything of value that an attacker, or threat actor, might which to exploit or from which they believe they can extract value. Paths include methods over which networks can be exploited to attack a target device or physical access to devices themselves.

- Sample attacks – Attacks are methods, some manual, some automated, used to find, identify, assess, and finally exploit target devices. These may be remotely executed across networks, using local access ports such as debug or USB ports, or physically accessing electronic components. Attacks may exploit protocol weaknesses or programming flaws.

- Motivations – Like all crime, there are many motivators for why attackers may wish to interfere with or otherwise hack and exploit a device. But, the key factors here are to assess what specifically attackers are trying to achieve in a technical context. This may be using the device to generate traffic for other attacks (such as denial of service attacks against another device), access private information, use processors or sensors for other purposes, or even maliciously interfere with a device to intentionally harm a random or specific individual.

- Mitigations – A wide range of methods may be used to limit, reduce, or eliminate attacks. Ultimately, the primary goal of most mitigation strategies must be to make exploitation of a given device expensive. This may be done through access controls implemented at or before the device in terms of traffic flow. Mitigations may be physical or logical, and may include operational security.

7.4 Assessment Methodology

Different threat vectors represent varying kinds and criticality of risks. There are many ways to assess risk. The Center has chosen a simplified model that is a synthesis of practices that also specifically addresses risk to patient. Risk will be categorized according to category, likelihood, and criticality (impact).

Categories of risk include confidentiality, integrity, availability, and risk to patient. These categories map to the foundational elements discussed in Section 8.5. Confidentiality includes the foundational security factors of authorization, privacy, association, and confidentiality. Integrity includes the foundational security factors of integrity, authentication, and lifecycle support (both service discovery and secure upgradability). Availability includes the foundation security factors of availability and lifecycle support (both service discovery and secure upgradability). The Risk to Patient category addresses unique security risks that may induce chance of injury or risk.

The likelihood of a threat resulting in an attack varies. The levels shown here are in keeping with [NIST-800-53], and are low, medium, and high. For purposes of the notional assessments provided in this technical report, the likelihood assumes a level of reasonable IT and network security at the hospital or care facility. This means that firewalls are put in place, all devices connected to the network are compliant to the security policy (for example, printers must also have reasonable device security). Of course, “reasonable” is a very nebulous term that may leave the leader lots of room for imagination.

The criticality is the level of impact to providing service. Levels are defined as follows:

- The potential criticality is LOW if: The loss of Confidentiality, Integrity, or Availability could be expected to have a limited adverse effect on customer operations, customer assets, or individuals.
- The potential criticality is Medium if: The loss of Confidentiality, Integrity, or Availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- The potential criticality is HIGH if: The loss of Confidentiality, Integrity, or Availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The risk assessment can be summarized as shown in Table 2.

Table 2: Threat Risk Assessment Summary

	Likelihood	Criticality
Confidentiality		
Integrity		
Availability		
Risk to Patient		

More comprehensive threat assessment modeling may be described in future iterations of this document. Also, these are only guidelines and examples of how to approach threat assessment at a very basic level. Meaningful assessment can only be done if threats and vulnerabilities are considered against each other in detail as they apply to specific use cases. This in turn provides a creditable basis to determine criticality and probability that is much more actionable than the generic process shared here.

7.5 Threat Assessment

7.5.1 Threat Actors in Cyberspace

It is important to consider the actors that may impact connected health systems. A sample table showing how threat actors can be identified and described is shown in Table 3. A more thorough consideration of threat actors that Members experience will be included in future versions of this document.

Table 3: Threat Actors in Cyberspace

Introduction

Cyber Adversary Situational Awareness: Nefarious cyber adversaries who are likely to target Smiths-Medical products and services consist of various groups. The Adsversary Taxonomy below details the various threat actor groups, motives, most probable & possible targetrs of opportunity, their cyber attack methodologies and associated compromise capabilities.

Nation State Cyber Capabilities & Motives:

1) Islamic Republic of Iran: Hackers are state sponsored, very nationalistic, and overall very dangerous and destructive in their targeting and capabilities.

2) People's Republic of China (PRC): Hackers are both state sponsored and criminal. Generally Chinese hackers are always very nationalistic. Their capabilities are stealthy, effective and enduring. Chinese hackers will most likely target intellectual property, operational procedures, prodcut design files. Cyber espionage is their forte and they are extremely effective. A burgeoning cyber criminal capability exists and is also a clear and present danger to multi-national enterprises.

3) Russian Federation: Hackers are primarily criminal, although the State will use these hacking capabilities for the projection of force in conjunction with internal Russian law enforcement efforts and countering external threats to the State using military cyber capabilities.

Cyber Threat Actor	Motive	Targets of Opportunity	Methodologies	Capabilities
Nation States – Peace Time	Economic, Military, National Secrets, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain short of kinetic
Nation States – War Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain including kinetic
Cyber Terrorists & Insurgents	Political	Infrastructure, Extortion and Political Processes	Combination of advanced persistent threats (APT)	A developing amd emergeing threat since 2012
Cyber Criminals – Grey & Black Markets	Financial	Intellectual Property Theft, Fraud, Theft, Scams, Hijacked Network & Computer Resources, Cyber Crime for Hire	Exploits, Malware Botnets, Worms & Trojans	Cell-based structure as an APT
Criminal Organizations – RBN	Financial		Use of above with distinct planning	Highly professional, dangerous
Rogue Organizations – Anonymous, LulzSec	Financial Military, National Secrets, Political Noteriety	Intellectual Property Theft, Direct & Indirect pressure on OGA Resources	Organic hacking capabilities unsurpassed	Organized yet de-centralized

7.5.2 Remote Access Threat Vectors

Remote access threat vectors leverage network access to attack a device. Five vectors have been defined for consideration.

1. WAN to Aggregation Point
2. WAN to Device
3. WAN to Service Elements
4. Hospital LAN/WLAN to Device
5. Hospital LAN/WLAN to Aggregation Point

These are illustrated in the following diagrams.

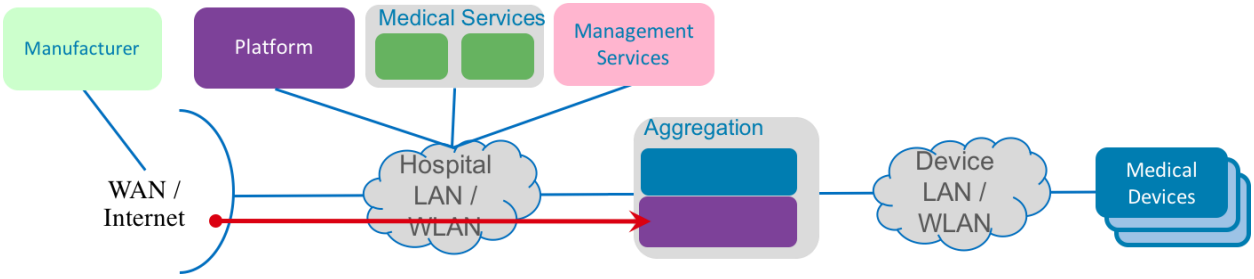

Figure 4: WAN to Aggregation Point Threat Vector

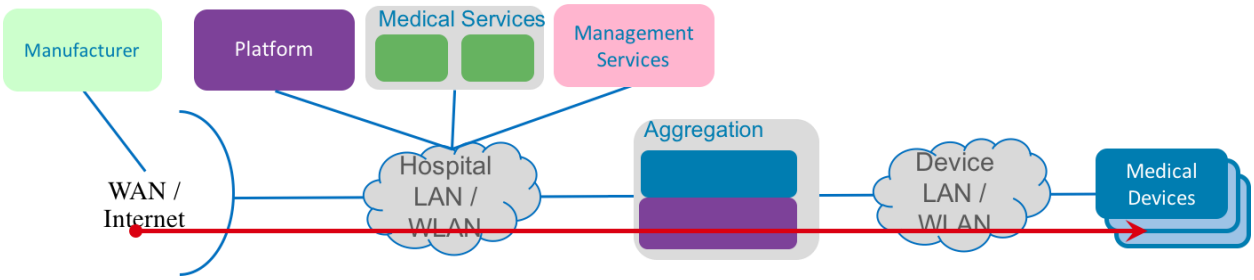

Figure 5: WAN to Device Threat Vector

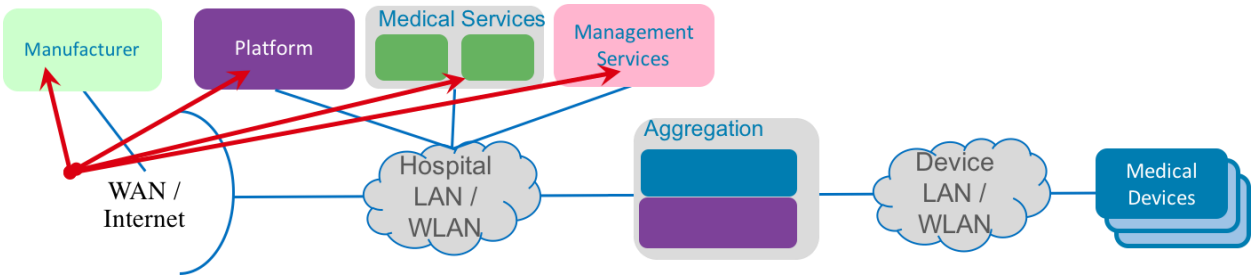

Figure 6: WAN to Service Elements Threat Vector

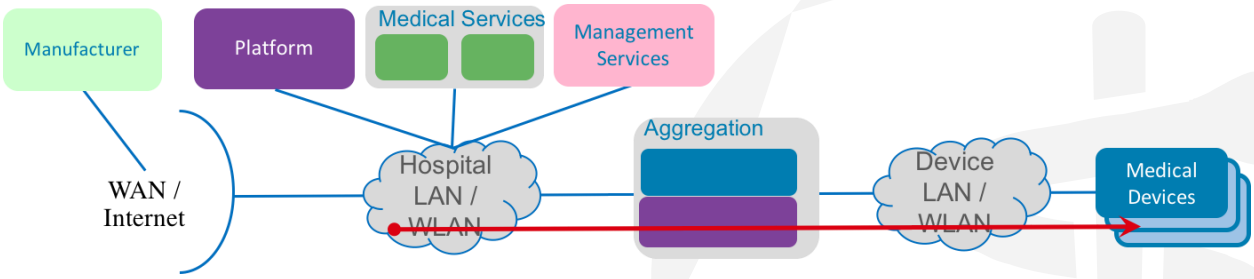

Figure 7: Hospital LAN/WLAN to Device Threat Vector

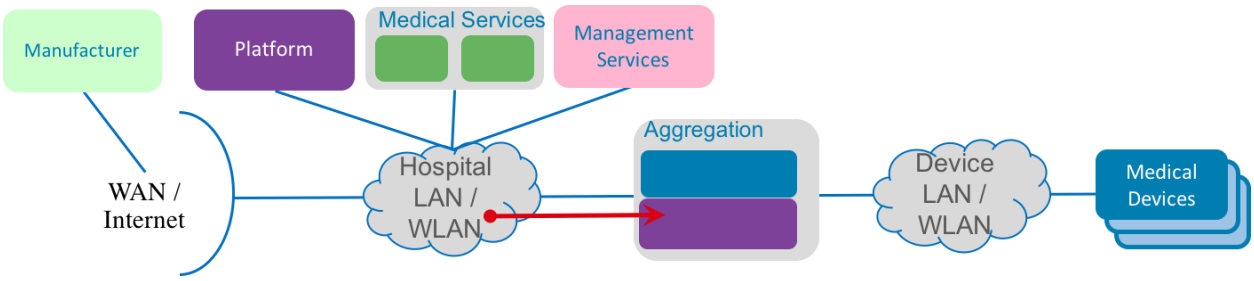

Figure 8: Hospital LAN/WLAN to Aggregation Point Threat Vector

Each of these vectors must be modeled and assessed according to the frameworks provided in Sections 7 and 8. This work will be summarized in a future iteration of this document. Also, there are other threat vectors. These may be added to future iterations of this document as well.

7.5.3 Network Threat Vectors

Attackers, with access to the network used by devices, may attack the communications between devices. This can be accomplished on virtually any network interface – WiFi, Bluetooth, or even wireless personal area networks (IEEE 802.15 including ZigBee, Thread, and many others) and wired connections. Wired communications can be accessed at the electrical or optical cable; they can also be accessed at routers and switches, and particularly at any location where frames or packets are on the edge (such as on an Ethernet bridge or hub). Given such access, an attacker may attempt to eavesdrop (snoop), modify, masquerade (spoof), or even directly access communications and devices. For example, an attacker may interject an evil interoperability platform and interfere with care or access private information. Future iterations of this document will address network threat vectors more completely.

7.5.4 Pivots

Often, attackers may remotely compromise one vulnerable device to access another device that would otherwise be inaccessible remotely. For example, an attacker may remotely exploit a vulnerable Bluetooth enabled thermometer to access an aggregation device. This is illustrated in Figure 9. Another example is an attacker may attack the thermometer and then pivot to attack another device on the subnetwork that was not remotely accessible from the location of the attacker.

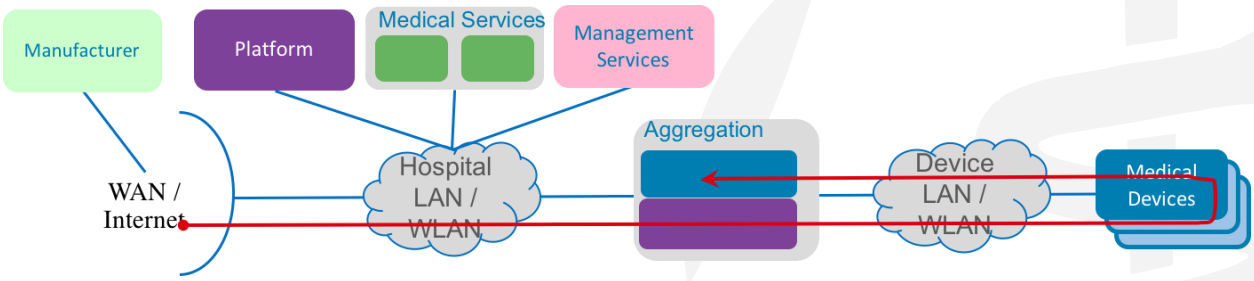

Figure 9: Pivot Threat Vector Example

There are many combinations of pivots that can be theorized. The critical aspect to accept about exploits that use pivots is that any network interface – WAN or LAN facing – can be a threat vector. That said, it may not be necessary to model and assess all pivot threat vectors if modeling and assessment of remote access threat vectors sufficiently address all interfaces.

7.5.5 Local Access Threat Vectors (Device Level Attacks)

Devices may be hacked locally, not just remotely. These are device level attacks. Within this technical report, this includes local access threat vectors include physical and device LAN access (since proximity is assumed). For example, potentially the device LAN may span across a hospital if it is built as a VLAN on a shared network. Such threat vectors assume what can attacked be after exploitation of the initial local compromise. As such, devices, aggregation points, and interoperability platforms must be modeled and assessed.

Motivations for local access threat vectors include those threats posed by Nation States during both Peace and War Time; Cyber Terrorists and insurgents; cyber criminals and cyber collectives such as Anonymous, Lulzsec, et al.

There is a variety of different types of cyber-attacks, specifically hacks through vulnerabilities in the electromechanical and software applications of devices. These include but are not limited to the following:

1) File Inclusion
2) Cross Site Scripting
3) HTTP Response Splitting
4) Denial Of Service (DoS)
5) Overflows
6) Escalation/Gaining Privilege
7) Directory Traversal
8) Bypassing confidentiality, integrity or availability

Future iterations of this document will address local access threat vectors more completely, including providing an illustrative reference architecture useful for discussing the threat vectors.

7.6 Threat Summary

After considering the threat environment discussed in this section, it is tempting to wax dramatic. That is not useful, of course. However, there are some key points to extract from the discussion.

First, there are many motivations and vectors for adversaries to attack devices – and those drive similar attacks against platforms and gateways and all the other elements of the hospital care infrastructure. Second, it is unlikely any combination of end point security controls, coupled with mitigating controls such as firewalls, will eliminate all threats – particularly as the threat environment is continually evolving. Consequently, it is essential to recognize that the hospital is, and will remain, a hostile cyber environment. Achieving interoperable infrastructure that provides data liquidity must address this reality.

8 The CMI Trust Framework

The foundation of CMI trust relies on PKI issued Certificates that immutably and uniquely identify connected components (devices, gateways, platforms, and other servers). However, implementing secure interoperability requires an entire framework of security techniques and practices. The framework includes:

- the security of the connected components themselves (notably devices and gateways),
- security associations between components at the link, network, and data liquidity layers,
- a PKI featuring certificates issued by an ecosystem Certification Authority,
- an overall security architecture.

These components of the framework are discussed in the following subsections. This is concluded with a discussion of how the framework applies the support to provide critical security functions.

8.1 Device and Gateway Security

Connected Devices and Gateways are complex. They incorporate sensors, processors, and information storage that leverage hardware, firmware, operating system, and common libraries. The device will also incorporate network interfaces, packet processing, and provide network application programming interfaces so that medical functions can access networks. Any of these functions or components is vulnerable to misuse or compromise, and so may leverage several security functions, components, or capabilities. Finally, the device must be managed and network and medical functions may have unique management requirements. Integrated as a whole, a notional anatomy is shown in Figure 10.

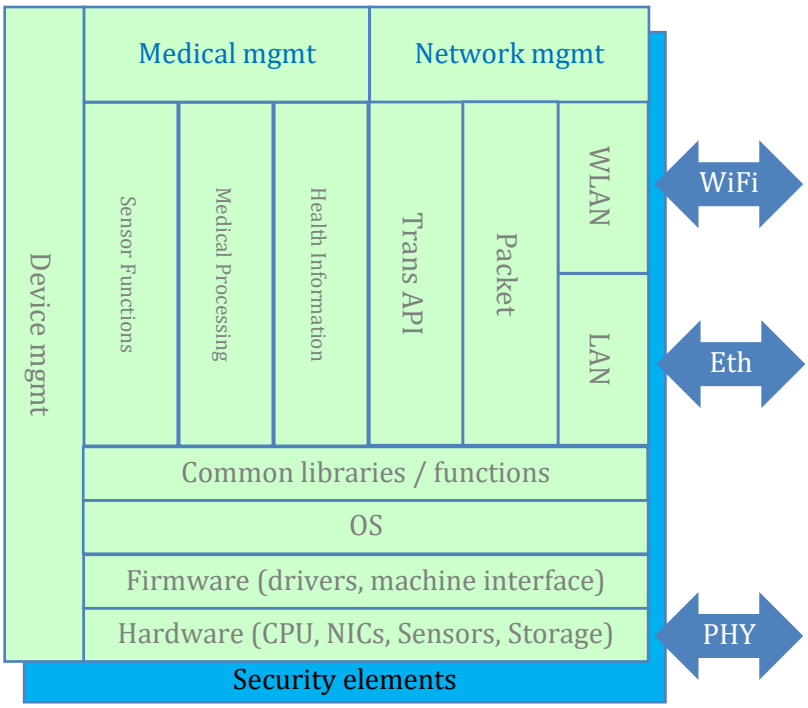

Figure 10: Notional Device Anatomy

The entire device needs to achieve an appropriate level of security. This includes several areas:

- Device security – Hardware should be hardened from tampering, including removal of manufacturer debug ports (such as JTAG or SPI). Firmware and drivers, operating system, and common libraries should be written using best practice secure software techniques. No unnecessary code or functions should be included on the device. Removable storage media ports or devices must be able to be disabled and, when enabled, must support access and other security controls. Devices must support typical security defenses such as anti-virus scanning and firewalls. Default passwords or other system backdoors will not be implemented.

- Network security – All network interfaces should support establishment of secure channels. Packet processing should be robust against malformed packets, fully compliant with the appropriate protocols such that no valid packet will cause denial of service or unauthorized remote access. Transport layer protocols will also support authentication and authorization, and provide for confidential communications and interoperability with peer and server devices. Anti-spoofing must be supported on any aggregation device. Default passwords or other system backdoors will not be implemented. This is particularly critical in Gateways and other aggregation elements. Gateways may also work as routers and service proxies that introduce additional opportunities for threats, and so must implement various security controls such as packet filtering, address translations, etc.

- Medical and health functions security – Medical and health functions may be integrated into the device in a modular fashion at the physical and logical (or possibly even virtual) level. Device

and network security principals listed above will also be implemented in these modular components, and any internal device application programming interfaces will also ensure that strong security functionality be applied to associations with other device components. Medical processing and functionality must be robust in operation, able to perform critical functions even when the supporting network is degraded. Personal health information must be protected according to regulatory requirements. Where appropriate, activities will be auditable and associated logs or records will be protected from tampering. Default passwords or other system backdoors will not be implemented.

- Medical, network, and device management – Management of medical, network, and device functions will implement strong security. All access must require authentication and authorization of activities and communications channels must be confidential. Authentication will implement a principal of privilege minimization. Software and firmware will be protected from tampering and only authenticated and authorized software will be used by the device. All changes or management interaction with any function on the device will be auditable, and associated logs or records will be protected from tampering. Changes of critical functionality or configuration will trigger alarms that are immediate reported using secure communications channels to appropriate management monitoring servers. Default passwords or other system backdoors will not be implemented. Gateways must be managed themselves, but also may be conduits through which Devices are managed. Gateways may be active in managing devices (often resulting in use of proprietary management interfaces not in scope) or may simply be transparent, relaying packets or messages to Devices.

- Security elements and functions – Security management will be executed at an even greater standard of implementation than the other security principals defined above. All changes or management interaction with any function on the device will be auditable, and associated logs or records will be protected from tampering. Changes of critical functionality or configuration will trigger alarms that are immediately reported using secure communications channels to appropriate management monitoring servers. System secrets and critical identifying information will be protected from unauthorized access and tampering. This will include, at a minimum, private keys and a unique device identity. Software and hardware implementing cryptographic processing will use government approved algorithms compliant with implementation guidelines (such as those provided by NIST in the United States).

All devices must adopt a principle of upgradable security. This means devices must be patchable and that security functions can be upgraded in the event that vulnerabilities are discovered. Software downloads should be attestable and secure. Where possible, device patching should be done automatically.

8.2 Security Association

One method to simplify the CMI architecture from the security perspective is to focus on specific types of security associations. Security associations apply multiple security techniques to achieve a

secure interface between communicating elements. The basic concepts are presented below and illustrated in Figure 11[2].

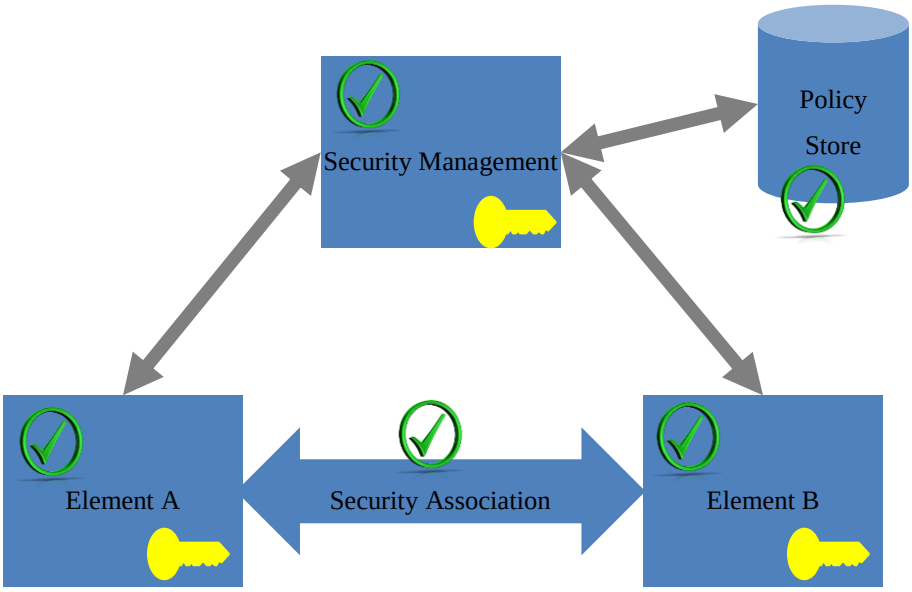

Figure 11: Security Associations

Security associations will be implemented based on the following principals.

- Based on strong identity: Identity is the basis for any meaningful trust system. Identity should be based on a secret paired with a unique identifier. The identity must be attested by a certificate or equivalent by signing or equivalent cryptographic operation. The certificate may contain other information (but not any information that should be changed such as software versions).
- Authenticated: Each security association must be verified when the association is requested using a cryptographic challenge.
- Authorized: Once entities have validated their mutual identities, their resource or activity accesses must still be authorized. Authorization should be based on a system or service wide policy system. The policy system should assume a least privilege orientation and assure separation of duty and function. Implementation may use a policy lookup or token grant approach.
- Isolated: Isolation of network, storage, and compute resources used for specific workloads must be assured. There are a wide range of obvious security risks that are managed this way,

[2] The notion of security associations as discussed here was presented in "Security of Open Distributed Architectures" by Steve Goeringer and Dr. Indrajit Ray at SCTE-ISBE Expo, 2017.

however, it is equally important from a performance perspective. Specifically, workloads or process should not impact other workloads or processes unless allowed by the operator. Isolation may be achieved by network segmentation (through secure addressing or encapsulation) and various virtualization tools for ensuring workload isolation in memory, CPU, and storage.

- Confidentiality: Data and communications should be kept private. The isolation functions discussed above may achieve sufficient confidentiality. However, encryption will ensure even stronger confidentiality, assuming adequate protection of encryption keys.

- Attested: Finally, all the security controls that implement a security association and protect it must be provably untampered. This is traditionally done using accounting and logging mechanisms. There are improvements in trusted computing systems that allow secure boot and run time monitoring to improve on legacy approaches. Whatever specific strategies are used, the goal must be to verify that the infrastructure and the security associations implemented to interconnect both hardware and software components are, indeed, what they are expected to be.

8.3 Defense in Depth

No security technique or strategy is perfect. To help ensure cost effective and practical security, security techniques should be applied recursively to achieve defense in depth. An analogy for discussing this approach is to refer to layers, though other words such as planes or levels or elements can be used in some other documents. Consideration of medical care infrastructure identifies at least six layers where security should be applied. The basic layers are the link, network, data liquidity, and management layer. Two additional layers should be considered as well – the internal and external data stores.

- Link layer: Directly connects components using wired or wireless interfaces. It is used by the network layer.

- Network layer: Overlays the link layer and provides for connectivity at a logical level across one or more links. Routing or switching may occur to achieve connectivity across multiple links. It is used by the data liquidity and management layers.

- Data liquidity layer: Usually, this is referred to as the application layer. However, in healthcare, this is too simplistic. Rather, the focus needs to be on the ability of applications to interoperate securely with information elements that are consistently formatted and interpreted by applications at various components.

- Management layer: Multiple management activities must be securely enabled at the link, network, and data liquidity layers. In some cases, management functions may be interconnected by data liquidity protocols or interfaces such as IHE PCD.

- Internal data store: A variety of patient, configuration, and management data needs to be stored on data stores in connected components. This is often referred to as local storage,

but in the age of cloud computing, local storage has broad interpretation. Here it refers strictly to data that is store at the gateway, device, platform, or other server.

- External data store: Gateways and platforms may need to access data that is remote from their local instance. This is referred to as an external data store. Note that some devices may also do so.

Each of these layers should implement security associations as discussed in the previous section. This creates a layered defense of nested authentication, authorization, encryption, and other controls. In this way, as discussed in the threat assessment, as adversaries compromise some elements of the infrastructure, they will not be able to simply pivot and exploit other elements. This layered approach dramatically increases the cost of attacking a healthcare infrastructure while assuring ease of operation and strong patient outcomes even as the care system is under attack.

8.4 Foundational Trust for Interoperability

The Center will achieve secure interoperability by implementing defense in depth using layers of security associations as reviewed in the previous sub-sections. The basis for trust in this strategy relies entirely on the strong implementation of immutable bindings between PKI certificates and their associated private keys.

8.4.1 Certificates

Public key infrastructure (PKI) anchors trust using certificates. Certificates will provide the basis for security associations; in other words, foundational security services including authentication, authorization, confidentiality (encryption), integrity, and non-repudiation. PKI provides a method to attest the validity of certificates as indexed by public keys. Subsequently, certificates and the execution of a robust PKI enable establishment of secure communications channels, storage of sensitive data, and management of devices including secure software downloads and upgrade. The Center will govern and oversee operation of the PKI as it relates to The Center's intended ecosystem. Certificates can be embedded securely in the device at manufacturing time, or may be loaded in the device by a certificate enrollment protocol such as Simple Certificate Enrolment Protocol [IETF-ID-SCEP].

8.4.2 Managed Certificate Authority

The Center will offer members and vendors a managed Certification Authority (CA) PKI. It will consist of a centralized CA hierarchy (including Root and sub-CAs) hosted by a trusted CA partner having experience with the secure operation of PKIs. Members and vendors will not be required to operate their own CA. Managed PKI services will include registration, validation, end-entity device certificate issuance, revocation services and PKI life cycle management. The center will issue and maintain a Certificate Policy specification that provides managed CA guidance and expectations. Implementation of the CA should be audited by a neutral third party to vet that the Certificate Policy is actually implemented.

Several alternatives to an ecosystem root have been considered. Many Center contributors believe each entity that installs identities should implement their own root (also referred to as self-signing). This solves supply chain risks in procuring roots and also leaves implementers fully in control of their own security risks. Multiple roots (sometimes referred to as self-signing). Two methods of leveraging multiple roots are known that achieves interoperability. Each component in the ecosystem can install certificates of the CA for any component they may need to communicate so they can chain certificates accordingly. The scalability of this solutions seems, at best, dubious. Moreover, it dramatically increases the likelihood that a CA or sub-CA has been compromised at any given time and any device issued certificates under that CA being vulnerable. This is a dramatic increase of the attack surface and should not be considered secure. The second solution is cross-certification whereby all CAs cross sign the certificates of other CAs they will allow to chain. This is more interoperable than the other scheme in run time, but introduces dramatic friction on the back-end operations of CAs. And, again, if any give CA is compromised, all cross-signed certificates are compromised as well.

8.4.3 Certificate Hierarchy

The Center's Root CA will anchor the certificate hierarchy. Sub-CAs will be designated. At least four classes of certificates will be supported, including Wi-Fi module, device, enterprise device, and application server certificates. This is illustrated in Figure 12.

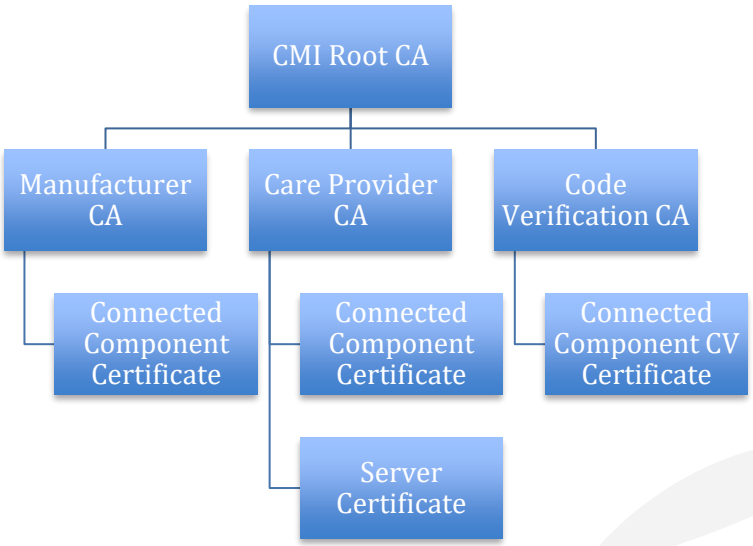

Figure 12: Center's Certificate Hierarchy

Integrating trust in this environment requires wide deployment of PKI certificates. Network access control will be required for both wireless and wireline access, the former being enabled by Hotspot 2.0 authentication and the latter being enabled by IEEE 802.1x access control. Device access to medical services and possibly other device functions may require separate certificates. Combined, this provides some defense in depth. An example of how this might work in a practical architecture

is shown in Figure 13. An implementation that requires a single certificate is highly desirable and The Center's initial specifications will be structured accordingly.

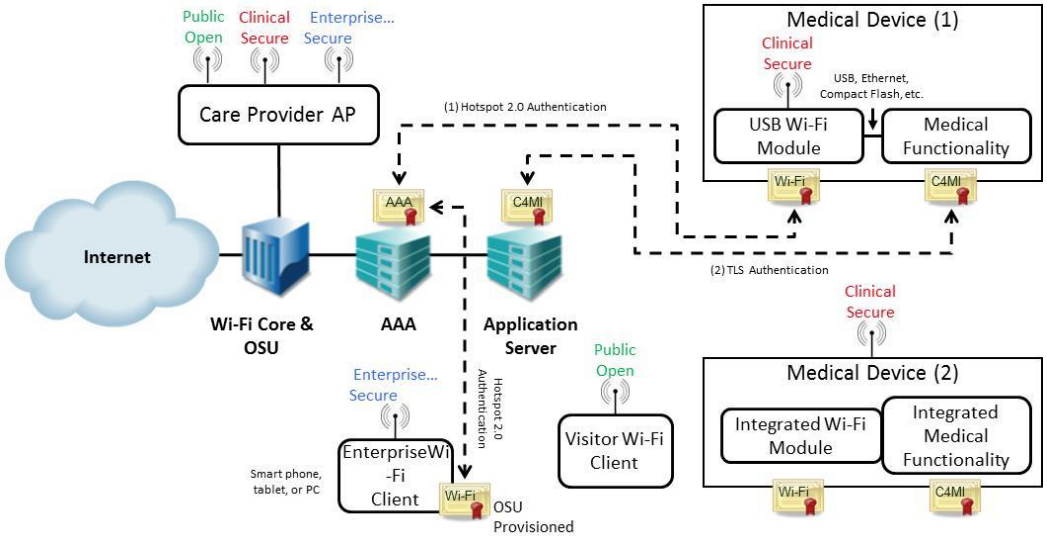

Figure 13: Certificate Locations on a Practical Architecture Using Dual Certificates

8.5 Foundational Security Elements

Certified security professionals know that achieving a secure infrastructure starts with applying well known fundamental principles. However, the execution of those principles can vary according to the domain and may involve unique requirements according to specific regulatory requirements and threats. The Center has identified several foundational elements as essential to achieve secure interoperable medical device connectivity. These are discussed in this Section.

8.5.1 Identity

Every connected device should have an attestable, immutable, and unique identifier. The Center will use PKI certificates paired with unique device identifiers. Devices may have different PKI-based certificates to support different roles (e.g. network functions, medical functions, administrative functions), but these must each pair to the devices' unique identity. Asymmetric cryptography provides the basis for attesting and immutability; and, therefore a basis for trust across the network of connected devices. This requires implementation of full PKI certificate lifecycle management, including certificate issuance and revocation policies.

Note that device identity and human identity are not synonymous. Secure administrator or caregiver identity must also be implemented. This can be based on PKI certificates, but other means may be more applicable depending upon specific use cases. Consequently, a secure API must be enabled to allow human access to protected device functions.

8.5.2 Authentication and Authorization

Interaction with devices must be authenticated, authorized, and accounted. Authentication will be based on presentation of identities which must be confirmed or verified. This will provide the basis for asserting policy based access controls to authorize use of functions and capabilities or changes of device configuration. All access to devices and their supported capabilities and changes of device configurations must be recorded and reported.

Specific device use cases will be considered in future iterations that consider the level of authentication and authorization required for safely operating devices. This will include emergency activities.

8.5.3 Integrity

The integrity of device processes, the information they produce and store, and the communications amongst devices must be assured. This includes assuring that device identities, execution environment, configuration, and communications are operating as expected and have not been altered in unauthorized ways. Messages between communicating parties should be verified as authentic and to be from the authorized sender and to the authorized received (message authenticity and non-repudiation).

8.5.4 Privacy and Confidentiality

Information stored on or communicated from devices must not be disclosed to unauthorized parties, devices, or processes. Sensitive information, such as Personal Health Information (PHI) or Personally Identifiable Information (PII), must be specifically identified and protected appropriately in motion or at rest. Stored information should be encrypted and secure communications channels (authenticated and encrypted) should be used for device connectivity.

8.5.5 Association

During care delivery, some devices should be strongly associated to specific patients. This can be referred to as patient to device binding. Attestable and accounted mechanisms of binding devices to patients must be provided. They must also be easy to use.

8.5.6 Availability

Like any area of information technology, not all devices are equally critical. Or, stated with greater precision, the critical nature of service provided by a device depends on the context in how it is being or may be used. A thermometer may not be as important, for example, as a blood pressure monitor. But, for a hypothermia victim, they may be equally critical.

Devices must be able to operate and provide essential functions even under network degradation such as DDoS. They should not be easily rendered unusable by unexpected traffic or traffic patterns. They must be counted to absolutely provide critical care to patients.

8.5.7 Lifecycle Support

Connected devices are very diverse. Some may be used frequently, others sparingly; some use technologies that are highly stable and mature while others require frequent software or firmware updates. Secure interoperability must provide support for ensuring that all devices are functioning when they need. Towards this end, to foundational considerations are service discovery and secure upgradability.

8.5.7.1 Service Discovery

Connected devices must be able to automatically connect to the appropriate aggregation, interoperability platform, management, and medical services devices. Device, network management devices, and human administrators must be able to discover what devices are on their network at any given time (which should also be auditable). Finally, caregivers should be able to discover the status and location of devices. However, device discovery processes enabling these use cases must not increase the vulnerability of devices or the networks over which they connect.

8.5.7.2 Secure Upgradability

Connected devices must be able to be updated securely. This includes providing support to upgrade the security on the devices. Secure software downloads should leverage The Center's PKI to sign, verify, and authorize software and firmware. The need to update devices should have a secure way to be orchestrated or signaled, and be responsibly executed (heart monitors should not be upgraded during surgery). Upgrades should be attested and accounted. Failed upgrades should revert to known working conditions.

Executing secure upgradeability consistently well in an ecosystem context, meaning with wide and consistent vendor support, will take time. Many vendors have excellent processes in place now and should be evolved carefully and deliberately as The Center's vision is realized. Consequently, secure upgradeability must be further expanded and addressed in future iteration of this document.

8.5.7.3 Secure Commissioning and Decommissioning

When devices are first turned on or brought into a network, service discovery will include executing necessary patching and establishing appropriate security protocols such that installation or configuration does not provide the opportunity for compromising the device. When devices are no longer necessary, certificates will be destroyed and added to appropriate records so they will be shown as invalid (such as a Certificate Revocation List, or CRL). Personal health information must be similarly destroyed.

9 Conclusion

This document introduces the trust framework and approach to security under development by The Center. This is based upon foundational elements and is enabled by extensive use of certificates as part of a Public Key Infrastructure (PKI). The Center feels this will be essential to achieving a widely interoperable and secure connected device ecosystem that safely meets the needs of patients and their caregivers.

Specifications and technical reports have been compiled to apply the concepts outlined here. These are:

- Identity Overview Specification – Specifies immutable and unique identity through use of PKI certificates for medical devices, gateways, interoperability platforms, and other servers that connect to these components.
- Certificate Policy Technical Report – Defines the certificate policy for the Public Key Infrastructure (PKI) used within the CMI ecosystem for implementation of Center CAs.
- IHE PCD Identity and Secure Transport Specification – Specifies requirements for securing IHE PCD HL7 MLLP messaging for North and Southbound interfaces reflected in the high-level architecture.
- Secure Automated Software Update Technical Report – Outlines trusted software update tracking requirements and presents interoperable functions for coordination of secure automated updates.

Other Center documentation may include additional security requirements and guidelines which are also derived from the principles and framework documented here.

This document is anticipated to improve over time. Further consideration to device security by design must be pursued. The roles of filtering, protection of secrets, techniques of assuring confidentiality and privacy, access, and authorization controls are topical areas that will likely modulate the security strategies outlined here. Moreover, a more thorough and complete threat assessment will be conducted. As the security framework evolves, additional specifications and technical reports will be developed, incrementally improving security interoperability.

Appendix I. Acknowledgements

The Center and its member companies would like to extend a heartfelt thanks to all those who participated in the development of this document.

Steve Goeringer authored this document. Special thanks to those who were directly involved via a variety of discussions, reviews and input: **Kai Hassing, Bill Hagestad, Stuart Hoggan** and **Ken Fuchs**.

This effort was conducted within The Center's **Security** Working Group, whose members have included the following part-time and full-time participants during the time period that we discussed this version of the document:

WG Participant	**Company Affiliation**
Andrew Dobbing	Laird
Bill Hagestad	Smiths Medical
Bill Pelletier	GE
Bo Dagnall	HPE
Bruce Friedman	GE
Doug Smith	Laird
Jay White	Laird
Jeffrey Brown	GE
Kai Hassing	Philips
Ken Fuchs	Draeger
Dr. Max Pala	CableLabs
Song Chung	Welch Allyn
Soundharya Nagasubramanian	Welch Allyn
Stefan Karl	Philips
Stuart Hoggan	CableLabs

- *Steve Goeringer (Security Working Group Lead), David Fann, Trevor Pavey, Sumanth Channabasappa; and, Ed Miller (CTO) -- The Center*