CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Technical Report
Foundational & Clinical Data Interoperability Overview

CMI-TR-OVERVIEW-D02-20190311

DRAFT

Notice

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-OVERVIEW-D02-20190311			
Document Title:	Foundational & Clinical Data Interoperability Overview			
Revision History:	D02			
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.

Trademarks

Contents

Figures

1 Introduction

The Center for Medical Interoperability is a 501(c) (3) organization led by members to positively impact how medical technologies work together. Specifically, The Center aims to improve information flow and make technology function seamlessly to achieve the best possible outcomes for patients. This goal of interoperability supports The Center's members' commitment to improve patient safety, care quality and outcomes, reduce operations complexity and cost, and minimize clinician burden and waste. The Center's members can be found on The Center's website (see Section 2.1).

This technical report summarizes industry efforts led by The Center to solve issues related to medical device interoperability to enable trust and data liquidity, i.e., an environment where data securely and seamlessly flows throughout the healthcare system. This is a first step towards accelerating the creation and adoption of care innovations and paradigms that will significantly improve clinical outcomes and care quality. System-wide data liquidity can enable the shift towards desired paradigms such as person-centered and value-based care. In these emerging models, an individual will be able to easily access relevant data, share it securely when and where required, be informed of how the data is being used, and benefit from resulting health rewards such as improved, personalized, care. The Center's members' will be able to verify data provenance, enable trusted data exchange within and across care settings, and be better advocates of individuals and patients.

This document is intended to be informative and recapitulates a set of specifications undertaken by The Center. Section 2 contains normative documents and specifications that include requirements for compliance, and additional informative technical reports. In addition, The Center provides a robust test environment to test and certify clients and other connected components for their conformance to the requirements in these specifications.

The Center's members and vendor participants are encouraged to refer to the latest versions of the documents listed in Section 2. These publications have been the result of collaborations facilitated by The Center and involving The Center's members and numerous healthcare ecosystem vendors. Authors, editors, contributors, working group members, and their affiliated organizations at the time of publication, are listed in the Acknowledgements Section of each document. Readers should note that this is the second revision of this draft document (D02), and as such aligns with second revisions of the documents listed in Section 2. The primary differences between D01 and D02 are: changes to the provisioning flow (addition of the client management entity), introduction of connected component profiles, client management, and standardized semantic terms for physiological monitors and mechanical ventilators.

The Center continues to facilitate iterations to the efforts outlined in this document, and additional initiatives not addressed in this document. For instance, The Center has initiatives in areas such as clinical care paradigms, value economics, ecosystem development, and industry adoption. Please

contact The Center (see Section 2.1) if you wish to obtain more information or to participate in these collaborative efforts.

2 Informative References

This technical report uses the following informative references.

The Center will be publicly releasing the D02 drafts of its documents referenced below later this year. Organizations who have signed an intellectual property rights agreement with The Center have access to these documents prior to the public release at http://bit.ly/CMID02Release (login required). Publicly released D01 documents are referenced below

[CMI-DOC-TD]	"Terms and Definitions", Center for Medical Interoperability https://medicalinteroperability.org/specifications/D01/CMI-DOC-TD-D01-20190311.pdf
[CMI-TR-F-SEC]	"Security Considerations for Foundational Efforts", Center for Medical Interoperability https://medicalinteroperability.org/specifications/D01/CMI-TR-F-SEC-D01-20190311.pdf
[CMI-SP-F-ANC]	"Access Network Connectivity Specification", Center for Medical Interoperability https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ANC-D01-20190311.pdf
[CMI-SP-F-PF]	"Provisioning Flows", Center for Medical Interoperability, Jan 2018 https://medicalinteroperability.org/specifications/D01/CMI-SP-F-PF-D01-20190311.pdf
[CMI-SP-F-ID]	"Identity", Center for Medical Interoperability, Jan 2018 https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ID-D01-20190311.pdf
[CMI-SP-CDI-IHE-PCD-IST]	"Clinical Data Interoperability using IHE PCD – Identity and Secure Transport Specification", Center for Medical Interoperability, Jan 2018 https://medicalinteroperability.org/specifications/D01/CMI-SP-CDI-IHE-PCD-IST-D01-20190311.pdf

[CMI-SP-F-ASUM] "Automated Secure Update and Management Framework Specification", Center for Medical Interoperability, March 2018

https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ASUM-D01-20190311.pdf

[CMI-SP-F-ASUM-MEM-DMC] "ASUM Solution for IHE PCD Clients Using MEM DMC", Center for Medical Interoperability, March 2018

https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ASUM-MEM-DMC-D01-20190311.pdf

[CMI-SP-CDI-IHE-PCD-SSE] "Clinical Data Interoperability Based on IHE PCD – Semantics, Syntax and Encoding," Center for Medical Interoperability, Jan 2018

https://medicalinteroperability.org/specifications/D01/CMI-SP-CDI-IHE-PCD-SSE-D01-20190311.pdf

[CMI-ORG-TWH] "Trusted Wireless Health: Requirements and Considerations", Center for Medical Interoperability, Sep 2018

https://medicalinteroperability.org/specifications/cmi-org-twh/CMI-ORG-TWH-D02-20180914.pdf

[IETF-RFC2131] "Dynamic Host Configuration Protocol"

https://tools.ietf.org/html/rfc2131

[IETF-RFC3315] "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"

https://tools.ietf.org/html/rfc3315

[HL7-FHIR] "Fast Healthcare Interoperability Resources"

https://www.hl7.org/fhir/overview.html

[WFA-HOTSPOT-2.0] Wi-Fi® Alliance Hotspot 2.0™ (Release 2) Technical Specification Package

https://www.wi-fi.org/downloads-registered-guest/Hotspot_2-0_%2528R2%2529_Technical_Specification_Package_v1-4_0.zip/29728

[IETF] The Internet Engineering Task Force, IETF®

https://www.ietf.org/

[IHE-PCD] "Integrating the Healthcare Enterprise (IHE) Patient Care Device (PCD)"

https://www.ihe.net/Patient_Care_Devices/

[IHE-PCD-MEM-DMC] IHE "Medical Equipment Management - Device Management Communication", Rev. 1.3 – Trial Implementation

https://www.ihe.net/uploadedFiles/Documents/PCD/IHE_Suppl_PCD_MEM-DMC.pdf

[HL7-MLLP] "Transport Specification: MLLP, Release 1"

http://www.hl7.org/documentcenter/public_temp_C1E5F025-1C23-BA17-0C523B8E9AF4EF38/wg/inm/mllp_transport_specification.PDF

[IETF-RFC1305] "Network Time Protocol (Version 3) Specification, Implementation and Analysis"

https://tools.ietf.org/html/rfc1305

[IETF-RFC5905] "Network Time Protocol Version 4: Protocol and Algorithms Specification"

https://tools.ietf.org/html/rfc5905

[IETF-RFC5246] "Transport Layer Security (TLS) Protocol, Version 1.2"

https://tools.ietf.org/html/rfc5246

[NIST-hRTM] "NIST RTMMS 'Harmonized Rosetta'"

https://rtmms.nist.gov/rtmms/index.htm#!hrosetta

2.1 Reference Acquisition

Center for Medical Interoperability (The Center), 8 City Boulevard, Suite 203, Nashville, TN 37209, USA;
Phone +1-615-257-6410; e-mail: info@center4mi.org; https://medicalinteroperability.org/

The Internet Engineering Task Force (IETF), IETF Secretariat®, c/o Association Management Solutions, LLC (AMS), 5177 Brandin Court, Fremont, CA 94538, USA; Phone: +1-510-492-4080; https://www.ietf.org/

Wi-Fi® Alliance (WFA), 10900-B Stonelake Boulevard, Suite 126, Austin, Texas 78759 USA; Phone: +1 512 498 9434; https://www.wi-fi.org/

Health Level Seven International (HL7), 3300 Washtenaw Avenue, Suite 227, Ann Arbor, MI 48104, US; Phone: +1 (734) 677-7777; https://www.hl7.org/

Integrating the Healthcare Enterprise (IHE), 820 Jorie Blvd, Oak Brook, IL 60523-2251 USA; Phone: +1 630-481-1004; https://www.ihe.net/

3 Terms and Definitions

This document relies on the terms and definitions specified in [CMI-DOC-TD].

4 Abbreviations and Acronyms

This document uses the following abbreviations and acronyms:

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EHR	Electronic Health Records
FHIR	Fast Healthcare Interoperability Resources
FQDN	Fully Qualified Domain Name
hRTM	harmonized Rosetta Terminology Mapping
IETF	Internet Engineering Task Force
IHE-PCD	Integrating the Healthcare Enterprise - Patient Care Device
IMM	Interoperability Maturity Model
MEMDMC	Medical Equipment Management Device Management
MLLP	Minimal Lower Layer Protocol
NTP	Network Time Protocol
PKI	Public Key Infrastructure
SDO	Standards Development Organization
SSID	Service Set Identifier
TLS	Transport Layer Security
WFA	Wi-Fi Alliance

5 Interoperability Principles

This Section provides The Center's definition of interoperability and the underlying principles, a model to qualify and achieve interoperability, and the scope of the efforts within this and associated documents listed in Section 2.

5.1 Interoperability Elements

Interoperability refers to the ability of connected components such as medical devices and-patient-care software applications to seamlessly exchange and make use of information. The following elements are deemed as critical for interoperability:

- **Plug-and-Play**: one can attach a client (medical device or a gateway) or system without requiring manual configuration of either side of the connection.
- **One-to-Many**: a client or system certified as being conformant with a set of specifications is now plug-and-play with similarly certified clients, systems, or both.
- **Two-Way**: data communicated between connected components can flow in both directions.
- **Trusted**: achieved when stakeholders are confident that interoperable systems are enabled to behave in a secure, safe, and reliable manner without unexpected behavior or failure conditions when built and tested according to specifications.
- **Standards-Based**: applying technical and health domain open standardized solutions to the overall medical interoperability reference architecture, interface specifications, and testing.

The intended result of the efforts to improve interoperability is data liquidity. This quick and on-demand trusted access to data - and associated information - by care team members, patients, and other authorized recipients enables better clinical outcomes, and person-centered care while reducing clinician burden.

5.2 Interoperability Maturity Model

The Center's members have offered an Interoperability Maturity Model, or IMM (Figure 1). This model speaks to the different facets that need to be addressed for interoperability: infrastructure, syntax, semantics, context, and orchestration. The intent is to iteratively address aspects of one or more of them over time.

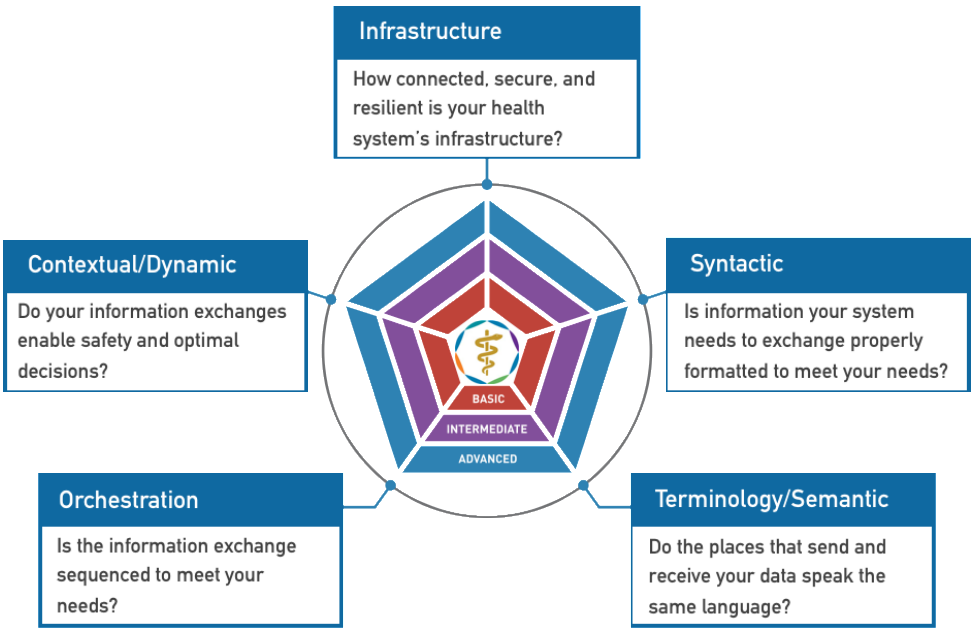

Figure 1-Interoperability Maturity Model

5.3 Current Scope

The Center's strategy for interoperability has multiple - iterative and parallel - stages to address foundational requirements, interoperability, scale, and transformational aspirations. The iterative approach is manifested in both the high-level architecture and the individual requirements for each iteration, based on the IMM.

Figure 2 showcases a highly-simplified, high-level architectural diagram with three layers. The client layer at the bottom includes devices, and gateways through which devices connect. They are collectively termed 'Clients.' The top layer contains applications, such as Electronic Health Records, clinical applications, and other innovative clinical solutions. The middle layer is a Plug-and-Play interoperability data orchestration layer that interfaces with the top and bottom layers. Collectively, these elements are termed Connected Components.

The scope of the initial efforts outlined in this document is to enable interoperability between the Client and platform services layers. This includes the following:

- Requirements and operational communications between the client and platform services layer to enable secure and seamless interoperability e.g., identity and authentication requirements, provisioning flows, secure software update, etc.

- Clinical data communications between the client and the platform services layer enabled via an Internet Protocol (IP) network

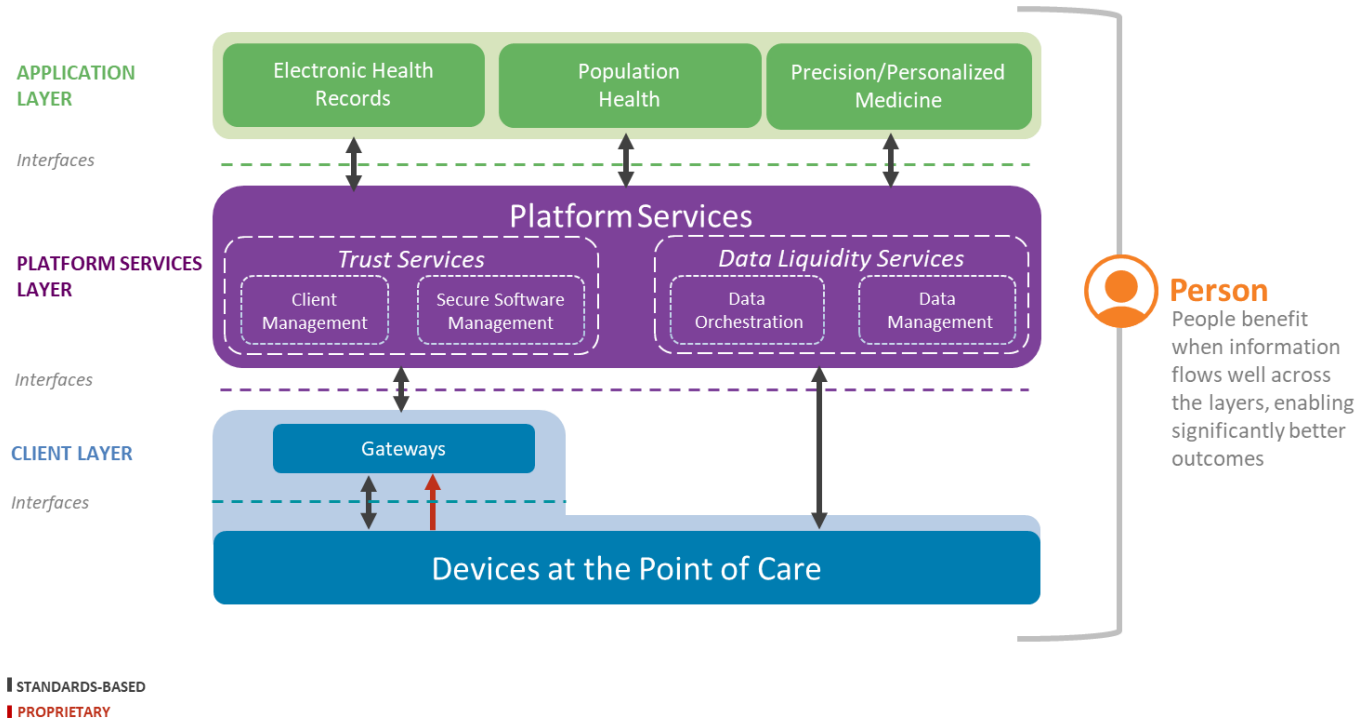

Figure 2-High-Level Architecture

The technical working groups facilitated by The Center continue to iterate on these efforts. Thus, the scope of the efforts summarized here should be viewed as an initial iteration and not the end goal.

6 Technical Overview

The compendious summary in this document can be broadly categorized into two areas:

- **Foundational**: initiatives independent of clinical data communications that are considered critical for secure interoperability, such as a trust model that specifies identifiers and identities for connected components, mechanisms to enable secure connectivity to wired and wireless networks, provisioning flows for automated participation in operational networks, profiles for automated and interoperable participation, a framework to remotely update software in a secure and interoperable manner (for instance, to enable quick, automated, responses to cybersecurity threats), and requirements to ensure architectural resiliency when unexpected conditions are encountered (e.g., errors in provisioning flows, or while sending clinical data).

- **Clinical Data Interoperability**: data communications between the Client and platform services layer related to patient care; this is based on existing standards such as [IHE-PCD] and Fast Healthcare Interoperability Resources [HL7-FHIR], extended as required to utilize the foundational elements such as the trust model.

Figure 3 visually illustrates the topics above. Both Foundational and Clinical Data Interoperability efforts aim to comply with the interoperability tenants in Section 5.1 and leverage the iterative IMM approach of Section 5.2. The current scope includes foundational, and clinical data interoperability based on [IHE-PCD] . Efforts based on [HL7-FHIR] for clinical data interoperability are not addressed in this version of the document.

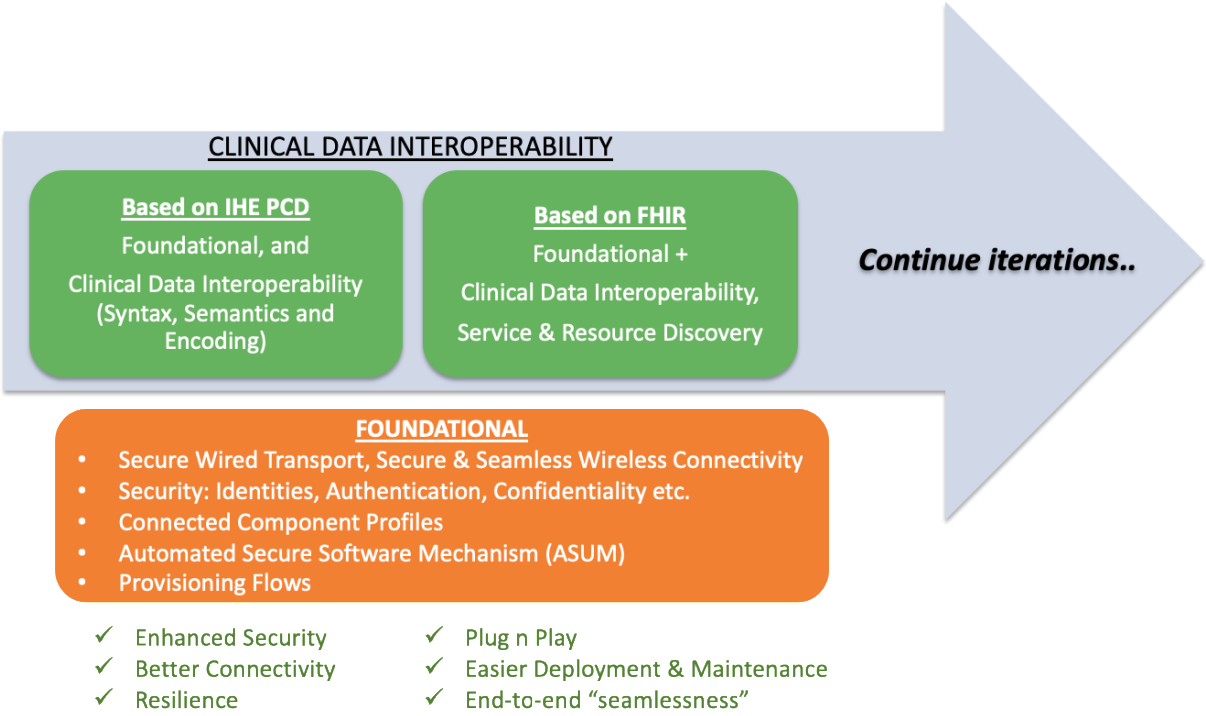

Figure 3-Foundational and Clinical Data Interoperability Efforts

The document map corresponding to the publications in Section 2 is shown in Figure 4. It distinguishes between normative documents and specifications, and informative technical reports. It also distinguishes Foundational and Clinical Data Interoperability efforts.

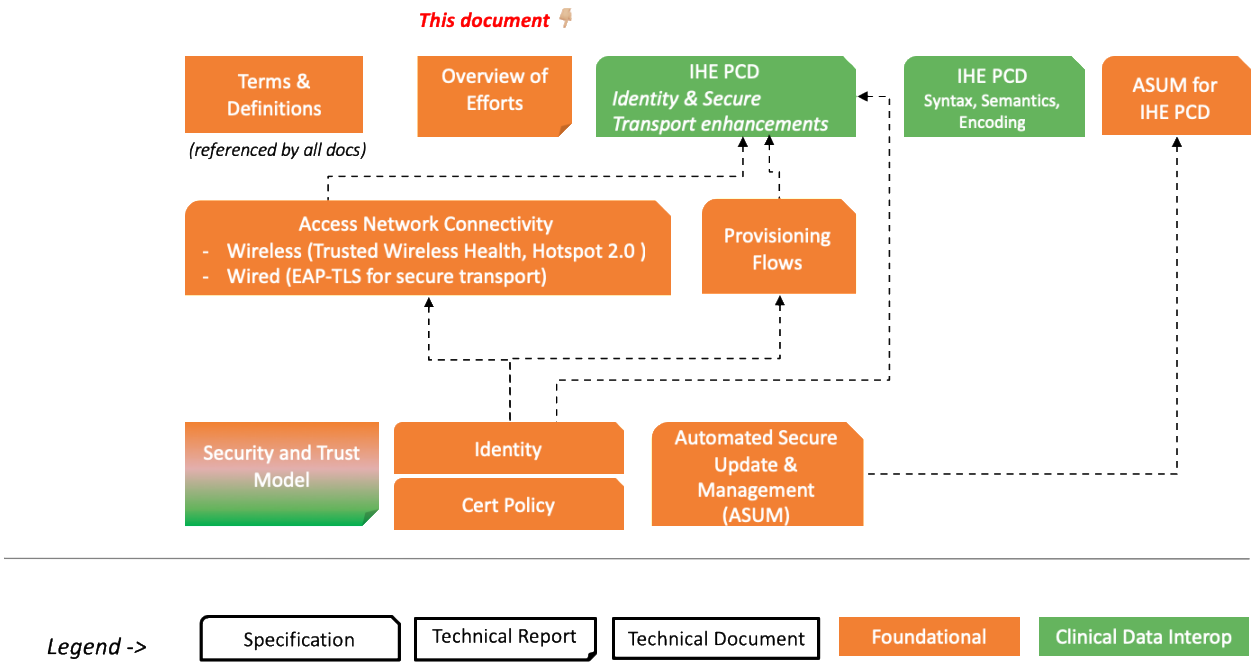

Figure 4-Foundational and Clinical Data Interoperability Document Map

6.1 Foundational Efforts

Foundational efforts currently address the following areas: security and trust, access network connectivity, provisioning flows, connected component profiles, and automated secure software update. In keeping with the expectations outlined in Section 5.2, the specifications leverage external standards wherever possible. In this iteration, most of the leveraged standards and protocols were developed within other specifications and standards bodies such as the [IETF].

6.1.1 Security & Trust

Security and trust are integral to enabling interoperability and trust. They are also critical to addressing cybersecurity threats. The Center's specifications address this architecturally via a trust model that includes key elements such as digital identities for connected components, mutual authentication for communications, and mechanisms for integrity and confidentiality.

Digital identities provide a clear and consistent way to identify and authenticate infrastructure elements: clients, platform services layer, applications, etc. To provide a basis for secure interoperability, these identities must be attestable by an ecosystem root of trust. They have associated identifiers for recognition and credentials for authentication. While identifiers and associated identities may be publicly shared, the authentication credentials are private. It is to be noted that authentication neither implies nor assumes authorization, which is separate and will need to be handled by health systems. Where appropriate, mechanisms for authorization are provided.

Identification via consistent identifiers and authentication is the first step towards trusting elements, such as clients and platform services layer. In addition, there is a need to ensure that data communications are kept confidential. To enable these elements, the security efforts specify:

- Digital Identities based on X.509 Certificates, via a Public Key Infrastructure (PKI) managed by The Center on behalf of the members and vendors that will be used to distribute digital certificates to compliant devices and member health system components
- Uniform identifiers
- Authentication protocols
- Digital signatures for integrity
- Encryption options for confidentiality

Identities enabled via Digital (X.509) certificates and PKI provide various desirable characteristics. For instance, conformant connected components that have never communicated before can authenticate each other without requiring any pre-configuration (saving time and effort), and private authentication credentials are never shared (increasing security). They can also be leveraged across the architectural interfaces such as connectivity, transport security, secure software download, etc.

Figure 5 illustrates the identity and authentication elements. Please refer to [CMI-TR-F-SEC] for a detailed overview of the security considerations, threat models to be considered, etc. For requirements related to identifiers and digital identities, see [CMI-SP-F-ID].

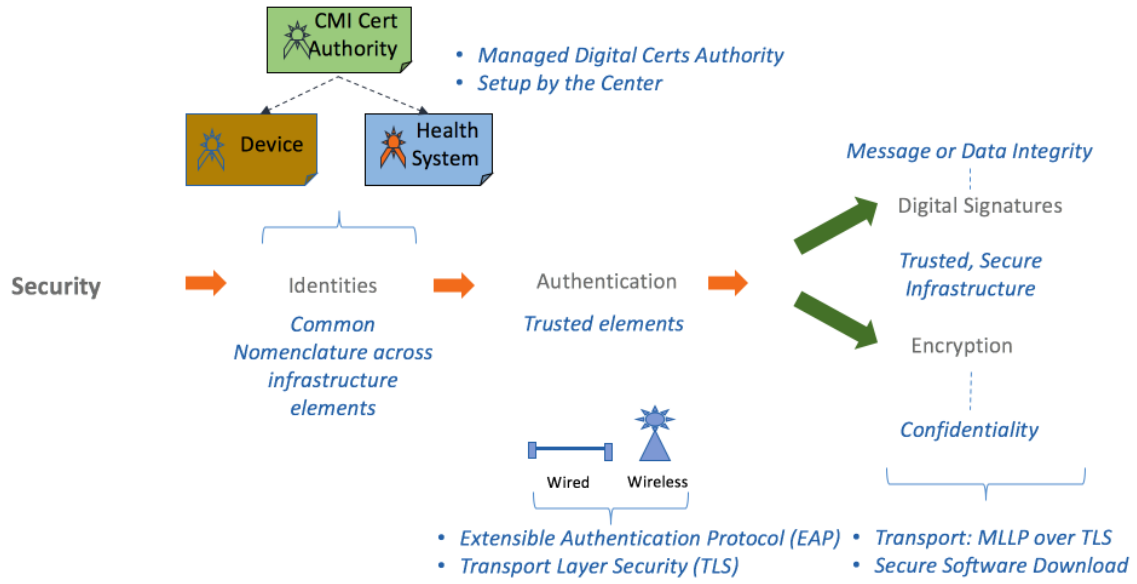

Figure 5-Security Solutions for Foundational Efforts

6.1.2 Access Network Connectivity

Wired or Wireless access networks enable connected components to communicate with each other and with other systems within a health care provider network. This allows the clients to discover and communicate with the platform services. The goal is to specify interoperable mechanisms that allow for seamless, consistent, and secure connectivity with improved performance (especially for wireless networks). This increases operational resilience, reduces deployment and operational complexity, and enables secure data transmission. Manufacturers benefit from being able to build, deploy, and replace products consistently across health systems. Health systems save time and resources with reduced operational complexity and fewer service interruptions. The improved security and performance contribute to trusted data liquidity, thereby improving care.

These requirements are documented in [CMI-SP-F-ANC], and address:

- Easy, zero- or minimal-touch connectivity
- Secure access network communications
- Better wireless performance, including roaming scenarios

Wired networks have an edge on wireless networks in that physical connections allow for straightforward access to the network. However, these connections must be secured to the same degree as wireless networks (see Section 6.1.3).

In many instances today Wireless networks require manual configuration of information (e.g., Service Set Identifier or SSIDs, credentials) on both the clients and the wireless access points for connectivity. This adds considerable time and effort for deployments (e.g., password creation on access points, password entry on multiple clients), complicates operations (e.g., when systems are upgraded, clients are replaced, passwords are changed) and adds security risks (e.g., due to simpler passwords or passwords that don't change).

To address this, the working group considered and selected the WFA's, which allows clients to discover and connect to access points without manual configuration of SSIDs or credentials. To use Hotspot 2.0, clients and access points should be able to mutually authenticate and utilize a uniform discovery mechanism. [CMI-SP-F-ANC] provides these by using the digital identities for clients and access points, and by specifying uniform realms (CMI or CMI_TWH). Thus, if a health system deploys conformant access points, then any compliant client (e.g., medical device or gateway) can automatically discover, mutually authenticate, and connect. It is to be noted that authentication is separate from authorization. Clients may be authenticated and may or may not be authorized to participate in a network. The health system will need to enable authorization via mechanisms provided by [WFA-HOTSPOT-2.0].

Wireless networks are also currently prone to performance issues, whether from resource constraints such as when non-medical and medical clients are placed on the same network, or when operations are interrupted due to roaming, or external factors that affect wireless connectivity. To this end, The Center has an effort – Trusted Wireless Health™ (TWH) - that aims to enhance performance and resilience for both clients and health system networks. [CMI-ORG-TWH] provides

operational guidelines and requirements for members. The client-specific requirements are included in [CMI-SP-F-ANC] and address the following, summarized in Figure 6:

- Efficient and minimally disruptive roaming across APs
- Methods to prioritize preferred traffic

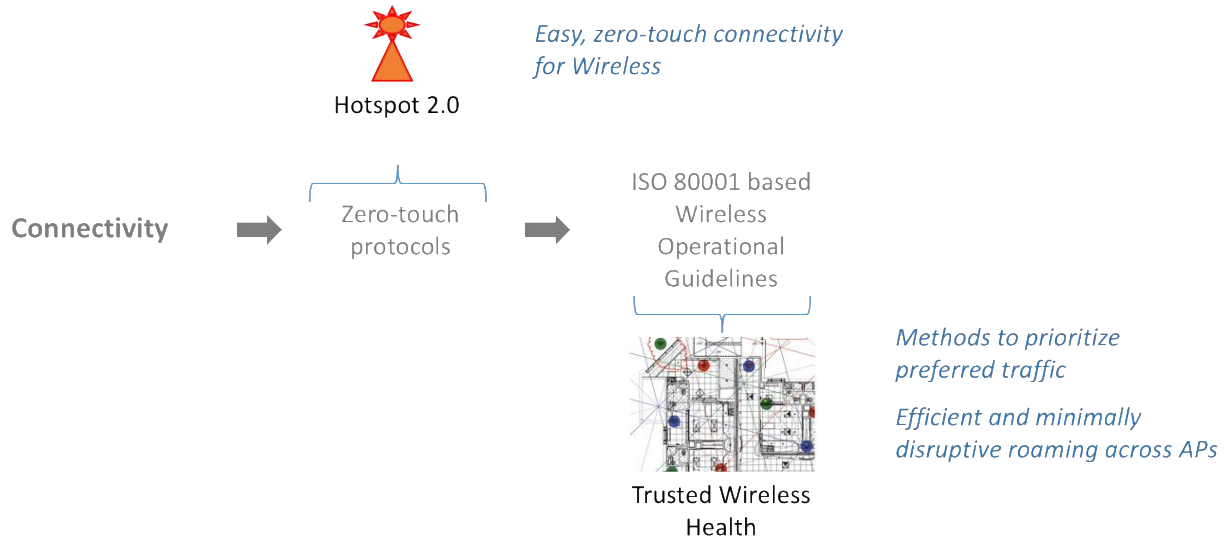

Figure 6-Connectivity Considerations for Foundational Efforts

6.1.3 Provisioning flows with Service Discovery

Provisioning flows, in this context, refer to the series of non-clinical-communications that a client undertakes prior to clinical data communications. In keeping with the interoperability guidelines (Section 0), the plan is to automate these steps in an interoperable manner. Within the current scope, the following steps have been specified:

- Access network connectivity: as described in Section 6.1.2.
- IP network connectivity: the client connects via internet standards track protocols [IETF-RFC2131] and [IETF-RFC3315] for IPv4 and IPv6, respectively.
- Initial configuration parameters: for the current scope, one of the key configuration parameters is a way to obtain time, which helps make data actionable for near-real-time communications and, in the long run, with data liquidity. This is accomplished via internet standards track protocols [IETF-RFC1305] and [IETF-RFC5905] for NTPv3 and NTPv4, respectively. In addition, to enable service discovery, two other parameters are required: Domain Name Server (DNS) and a domain name. The NTP server, DNS, and domain name are all made available via DHCP.
- Service discovery: broadly, this covers the identification of connected components that provide specific services such as data communications or management. For the current scope, the client starts by discovering a Client Management Entity. Once the client mutually

authenticates with the client management entity, it is informed as to whether it is authorized, or not. Independent of authorization status, the client management entity may direct the client to an Automated Secure Update Mechanism (ASUM; see Section 6.1.5) management entity to attempt a software update (e.g., if that's the reason it is not authorized). If the client is authorized the client management entity will provide the platform services layer information for clinical data communications. The service discovery for the client management entity is accomplished by using this prescribed hostname - "CLIENT_MGMT_ENTITY" and combining it with the default domain name (from DHCP) to form a Fully Qualified Domain Name (FQDN) that is then resolved via DNS. The ASUM management entity and the platform services addresses are delivered as FQDNs via the client management entity. The use of DNS utilizes Internet-standard practice to allow for dynamic configuration of network entities, allowing for quick restoration of services when specific IP endpoints become non-operational, for load balancing, etc.

The Provisioning flow for a compliant client is showcased in Figure 7. Exchanges with the ASUM management entity and the platform services are not shown. The requirements related to this can be found in [CMI-SP-F-PF].

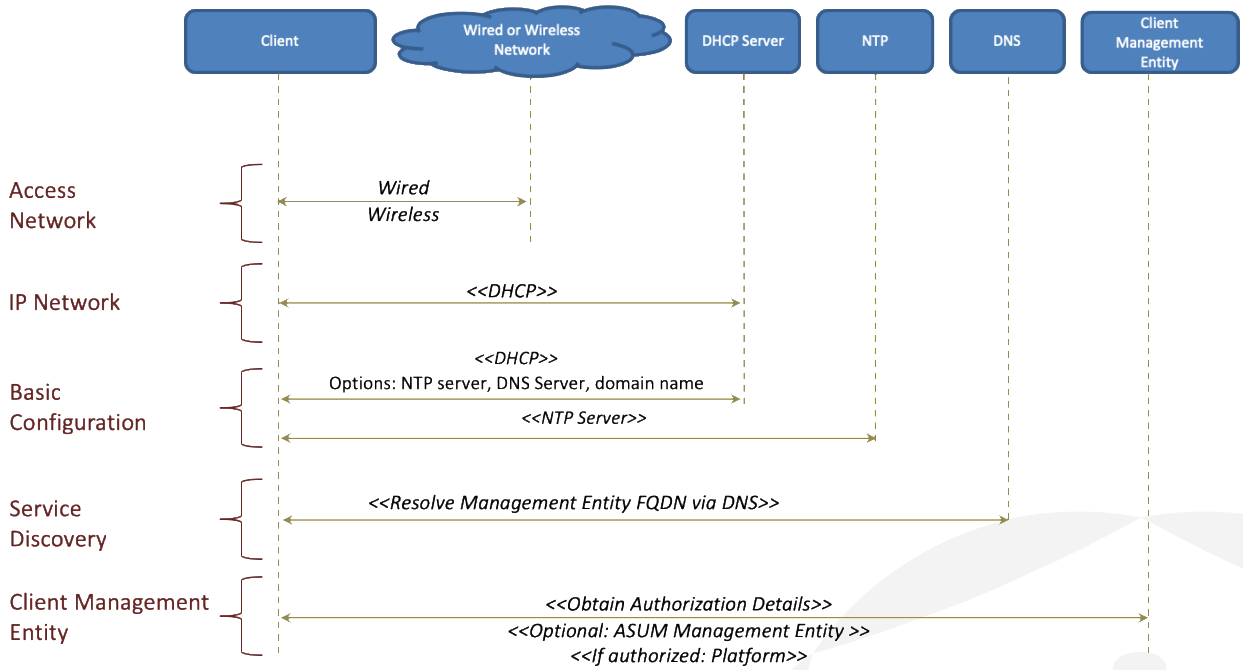

Figure 7-Client Provisioning Flow

6.1.4 Release Bundles and Connected Component Profiles

6.1.4.1 Release Bundles

The service discovery mechanisms specified within provisioning flows (Section 6.1.3) enable connected components to establish secure communication channels, but meaningful data exchange across those secure channels requires more. Components that comply with the same version of this

architecture will be aligned by definition, but the architecture will evolve, and while backwards compatibility is desired, it may not always be feasible.

To support 'Plug-and-Play' interoperability (see Section 5.1), a *Release Bundle Version (RBV)* indicates which version of the architecture a connected component complies with. The RBV follows standard "MAJOR.MINOR.PATCH" semantic versioning practices, where a new minor version indicates maintained interoperability, and a new major version indicates interoperability cannot be guaranteed.

Note that a connected component may comply with multiple versions of this architecture. For example, a Client Management Entity may wish to support older Clients, so it advertises multiple RBVs.

6.1.4.2 Connected Component Profiles

A *connected component profile* provides a mechanism for components to exchange release bundle identifiers and other metadata to support automated compatibility recognition, protocol negotiation, and smooth communications. This profile is a machine-readable description of a component and its capabilities and is exchanged at run-time between connected components in various scenarios. For example, when a Client first connects with a Client Management Entity, the Client sends its profile, and the management entity responds with its own, enabling automated verification of communication compatibility and (potential) fallback to a mutually supported protocol.

The metadata associated with a connected component could be quite large. For efficiency, the profile is split into a Minimum Connected Component Profile (MCCP), which contains the elements needed for baseline interoperability, and the Connected Component Profile (CCP), which contains all other associated metadata. The MCCP is always exchanged when two components attempt communication; the MCCP contains a link to the CCP for run-time querying as needed.

6.1.5 Automated Secure Update Mechanism (ASUM™)

ASUM addresses how medical gateways and devices can be identified and managed for software updates. It includes a foundational ASUM framework that specifies the base requirements for interoperability. Solutions conformant to this framework are then specified using clinical data protocols. As of this publication, a solution has been specified based on [IHE-PCD]. Future iterations will consider other protocols, such as or [HL7-FHIR].

The ASUM framework specifies components that address the benefits summarized in Figure 8.

Figure 8-ASUM Benefits

These are accomplished via a set of specific requirements:

- Clients share essential details such as model, identifier, software version etc. over a communications channel, which will automate remote inventory management and avoid manual location and inspection of medical devices and gateways to collect such information.
- Uniform software update trigger mechanism that can be sent remotely to any Client, to enable quick, remote, actions independent of vendor or model, e.g., in response to cybersecurity threats.
- Clients always authenticate software images so that the update process can be trusted and does not in itself increase threats; authentication may be provided by the manufacturer, and optionally via the health system.
- A set of failure conditions are identified so that clients can recover from common errors automatically and avoid manual intervention for recoverable conditions; examples include erroneous software images, inability to authenticate, etc.
- The framework and the specific solutions are themselves extensible, e.g., for additional failure conditions, additional security requirements etc.; the solution itself can be used to not only address cybersecurity threats but also to provide timely feature updates.

All of the above need to be supported as specified for compliance, with one exception. The ASUM framework allows for clients to download software securely via a specified mechanism or use an alternative solution as long as it meets specific transport security requirements around mutual authentication and integrity.

Software updates can be disruptive when medical devices and gateways are in use. To allow for this, ASUM assumes that updates are pre-scheduled. When a trigger is sent the client may optionally be allowed a time period (e.g., 1 hour, 4 hours) to attempt an update, or to reject the update if it is in use and the client is aware of it. A visual overview of the ASUM specified flow is shown in Figure 9.

As for scope, the current iteration, this applies to IP-based gateways and devices that connect directly via Internet Protocol (IP). Please refer to [CMI-SP-F-ASUM] for the ASUM framework and associated requirements, and [CMI-SP-F-ASUM-MEM-DMC] for a framework conformant solution using [IHE-PCD-MEM-DMC].

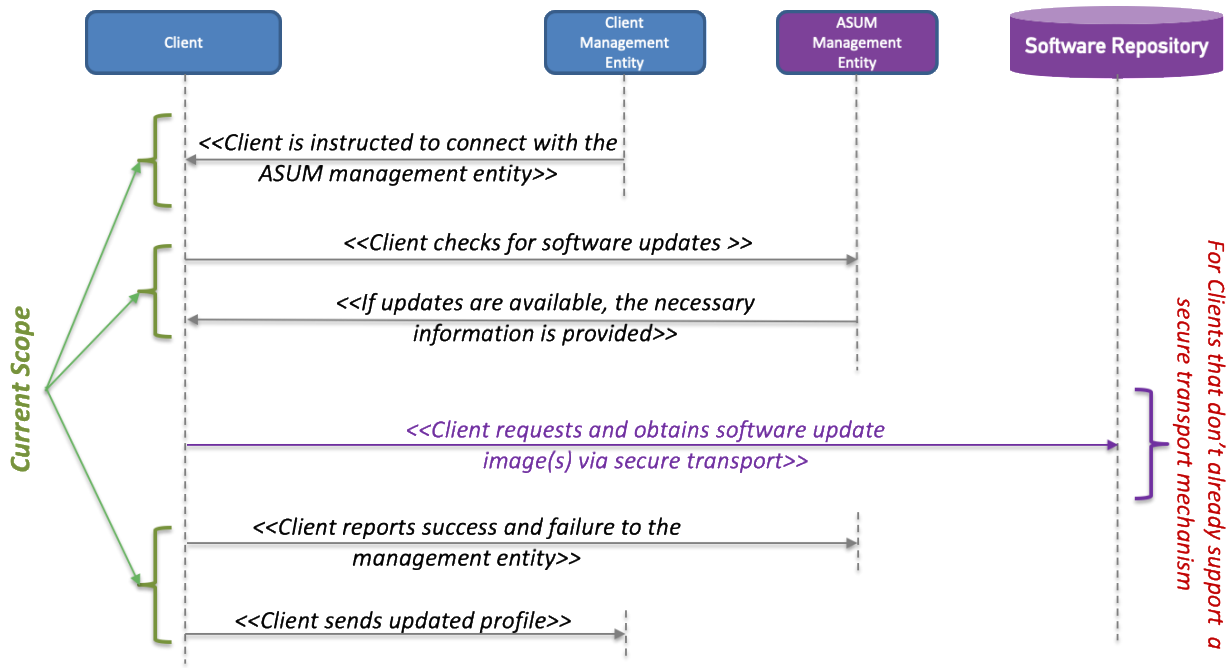

Figure 9-ASUM Flow

6.2 Clinical Data Interoperability Efforts

Many existing domain-specific clinical terminologies represent years of thoughtful subject matter expertise and a proven record of maintenance by well-established SDOs. Similarly, the HL7 2.x messaging protocol is foundational to data transfer across the healthcare industry. More recently, the emerging use of integration profiles and specifications such as, [IHE-PCD] and [HL7-FHIR], target interoperability through the coordination and specification of existing semantic standards. Without subtracting from these or sacrificing information integrity these foundational resources are leveraged as the source definitions and messaging syntax in a functional domain of interest. Targeting a subset of the selected domain can focus interoperability on prioritized clinical concepts.

Efforts began with measures of cardiovascular function, lung mechanics, and core biometric signals. Because The Center's origin was grounded in a critical-care demand for device interoperability, biometrics compromising the extracorporeal extension of physiologic interoperability were targeted. These important indicators of moment to moment patient status are easily accessible, rich in signal information, and highly significant from a clinical perspective.

Because patient and clinician confidence are dependent on reliable clinical data, targeting user confidence through interoperability is essential. The following imperatives as a part of CMI's clinical data interoperability specifications warrant clinical data as interoperable when delivered across a trusted platform:

- Defined semantic priorities: Clinical subject matter experts sourced by member organizations prioritize clinical concepts and constrain the associated semantic space from currently existing standards. Feedback is provided to the contributing SDOs regarding gaps in clinical concepts or support for disambiguation.

- Identification of representative use cases: Member organizations identify relevant clinical use cases representing commonly encountered clinical concepts and/or identification of opportunities for transformational clinical care models. Targets emphasize patient safety, clinical quality, interventional outcomes and workflow efficiency in order.

- Client engagement: Participating clients are engaged, and feedback is solicited on review of clinical priorities and use case modeling.

- Demonstration of conformant semantic interoperability: Semantic interoperability must be reproducibly demonstrated through conforming identification and representation of physiologic signals, biometric data and structured documentation of targeted clinical concepts.

- Underlying foundational requirements: Clients are required to support the security, connectivity, and provisioning flows as indicated in Section 2. In addition, clients that are Gateways, or devices that connect directly to the platform services, are required to support ASUM as specified in [CMI-SP-F-ASUM].

- Secure transport: to ensure end-to-end security the data transport has been enhanced via [IETF-RFC5246], which uses digital identities as specified in [CMI-SP-F-ID]. Refer to [CMI-SP-CDI-IHE-PCD-IST] for the associated requirements.

By way of example, the semantic interoperability of medical device data exchange is achieved by restricting [IHE-PCD] transactions to a CMI-defined subset of the [NIST-hRTM] terminology. The semantic space so defined includes observation types, units-of measure, measurement sites, etc. Rather than tackle an entire clinical domain, this effort is defined by member clinicians and other subject-matter experts and organized by functional domain constrained by clinical concept and driven by clinical use-case design and would include devices such as a physiologic monitor or ventilator.

These [IHE-PCD]-based transactions within a CMI-constrained terminology comprise a data model for the unambiguous exchange of clinical data between clients and the Medical Interoperability platform Services. The full set of requirements ensuring interoperability across semantics, syntax and encoding can be found in [CMI-SP-CDI-IHE-PCD-SSE].

6.3 Resiliency

The technical overview thus far has focused on ideal conditions where no errors are encountered. For instance, the client connects securely to the access network, executes the provisioning flow, is authorized by a management entity, initiates data communication with platform services, and securely updates its software when instructed by an ASUM management entity.

In reality, the client and connected components may encounter various errors such as inability to resolve the management entity from the DNS (e.g., due to misconfiguration), authentication errors (e.g. due to expired certificates), data transmission errors (e.g., network congestion, platform service errors), etc. In order to meet the Plug-and-Play and Trusted aspects of Interoperability (see

Section 5.1) the architecture needs to anticipate such errors and provide guidance to the connected components on remedial steps they can take to recover. This is done as part of *Resiliency* related additions.

As part of these Resiliency addendums an initial set of errors and warnings are identified, and remedial steps provided. In addition, such conditions are associated with event codes. These can be saved as logs, or sent as events (e.g., clients to a management entity).

7 Adoption and Operational Considerations

The CMI architecture outlined in this document presents an initial iteration of plug-n-play, one-to-many, two-way, trusted, standards-based, medical interoperability. Deployment of components compliant with this architecture can provide advantages such as: security and trust enabled throughout the architecture, ability to create an automated inventory of devices and gateways to manage secure updates and other purposes (e.g., deauthorization), resilient operations, consistent data communications, etc. The end result can be significantly easier deployments, smooth operations, and secure data liquidity across the architecture. This can enable and support multiple care paradigms including person-centered care.

Operationalizing this requires adoption and implementation by vendors, and procurement by healthcare providers. Assuming a marketplace of compliant products, there are additional operational complexities to consider. While new provider instances (e.g., hospitals) may deploy compliant architectural components from the beginning, most existing provider instances adopting this architecture are expected to migrate to this architecture over time. The latter presents complexities, such as security and trust and data liquidity in a mixed environment. To assist with this, one proposal is to consider such a migration in stages. One such approach is indicated in the following sub-sections.

7.1 Security and Trust

Planning for identifiers, identities and authentication across interfaces is the first step towards secure interoperability. In a mixed legacy and CMI-compliant environment it will be critical to understand authentication and authorization and their impact on operations. This can include a planned migration from a myriad set of identities (e.g., passwords, siloed digital certificates) to an industry-PKI based mechanism. This may also require additions to the current architecture to allow for cross-authentication mechanisms that are beyond the scope of this document.

7.2 Backoffice components for provisioning flows

Given that automation and resilience of operations is a key part of this architecture, a few well-established back-office elements and standards have been incorporated. These include DHCP, NTP and DNS servers, and the associated protocols. In addition, a couple of new elements based on healthcare standards have also been included. These are the Management entity, the ASUM management and a platform Services. Incorporating these prior to onboarding compliant components will accelerate the onboarding process for compliant components.

7.3 Secure software updates

Compliant connected components will support ASUM for secure software updates. This can be a critical feature to keep the clients updated as required to protect from cybersecurity threats. In addition, it may also help with general and feature updates from vendors.

7.4 Access Network Security

Automated access network security is included in the architecture. Current legacy networks may already have compensating controls to allow for this. To migrate to compliant interfaces, additional components are required. For instance, wireless network security requires compliant wireless hotspots and AAA servers. The AAA servers may be able to use current compensating controls (e.g., whitelists or blacklists) for this purpose.

7.5 Additional considerations

One of the challenges of having a mixed network with legacy and compliant connected components is the separation of datasets if secure data liquidity is a goal. Keeping track of data that is sent from compliant, mutually authenticated interfaces, from legacy components can be a tricky in a mixed environment. Future additions to the CMI architecture may assist with this by providing data-marking capabilities. Such extensions may allow connected components to validate if they received data over compliant interfaces that were mutually authenticated.

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. We also note that Dr. Bill Stead (Vanderbilt University Medical Center) authored the IMM.

Sumanth Channabasappa was the primary author of this document. Special thanks to those who were directly involved via a variety of discussions, reviews and input: **Steve Goeringer, Bernie McKibben, Ken Fuchs, Daymon MacCartney** and **Trevor Pavey**. For the D02 version of this document, additional contributions were made by Dr. Richard Tayrien and Spencer Crosswy (Clinical Data Interoperability) and Bowen Shaner (access network connectivity). David Fann, Chris Riha, and Trevor Pavey provided additional comments and suggestions. Christie Poland, Joan Branham, Katy Hoyer and Jessie Hanson have served as editors for the D01 version of this document. Jessie Hanson edited this version.

Chris Riha is the CMI Lead for this document. This document was primarily discussed and reviewed within The Center's **Architecture and Requirements** Working Group, with additional input from the Security and Connectivity Working Groups. The part-time and full-time working group participants, additional offline reviewers, and their affiliations are listed below:

Working Group Participants	**Company Affiliation**
Aishwarya Muralidharan	vTitan
Alex Poiry	Cerner
Ali Nakoulima	Cerner
Andrew Meshkov	86Borders
Brian Long	Masimo
Brian Scribner	CableLabs
Bruce Friedman	GE Healthcare
Corey Spears	Infor
Darshak Thakore	CableLabs
David Hatfield	Becton Dickenson
David Niewolny	RTI
Eldon Metz	Innovision Medical
George Cragg	Draeger

Working Group Participants	Company Affiliation
Guy Johnson	ZOLL Medical Corporation
Ian Sherlock	Texas Instruments
James Surine	Smiths-Medical
Jason Mortensen	Bernoulli Health
Jay White	Laird
Jeffrey Brown	GE Healthcare
JF Lancelot	Airstrip
John Barr	CableLabs
John Hinke	Innovision Medical
John Williams	FortyAU
Kai Hassing	Philips
Ken Fuchs	Draeger
Logan Buchanan	FortyAU
M Prasannahvenkat	vTitan
Massimo Pala	CableLabs
Mike Krajnak	GE Healthcare
Milan Buncick	Aegis
Neil Puthuff	RTI
Neil Seidl	GE Healthcare
Ponlakshmi G	vTitan
Scott Eaton	Mindray
Stefan Karl	Philips
Travis West	Bridge Connector

- *Sumanth Channabasappa (Chief Architect), Steve Goeringer (Security Architect), Chris Riha (Working Groups Lead), Paul Schluter, Bowen Shaner, Jacob Chadwell, David Fann, Spencer Crosswy, Dr. Richard Tayrien, Trevor Pavey; and, Ed Miller (CTO) -- The Center*