CENTER *for* MEDICAL
INTEROPERABILITY

The Center for Medical Interoperability Document Terms and Definitions

CMI-DOC-TD-D02-2019-05-31

Draft

Notice

This document 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.

Table of Contents

Document Status Sheet

Document Control Number:	CMI-DOC-TD
Document Title:	Terms and Definitions
Revision History:	D02 IPR Review
Date:	04/01/2019
Status:	Draft
Distribution Restrictions:	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 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 documents are subject to the Engineering Change Process.

Closed A static document, reviewed, tested, validated, and closed to further engineering change requests to the document through The Center.

1 Scope

1.1 Introduction and Purpose

This document establishes Terms and Definitions for use within The Center's efforts and documents. The principal intended reader of this document is expected to have a basic understanding of clinical informatics.

1.2 Requirements

This document specifies terms and definitions that will be normatively or informatively referenced by other documents. As such, this document, in itself does not specify requirements.

2 References

2.1 Informative References

This document uses the following informative references:

[HL7-FHIR-RD] "FHIR Resource Device - Detailed Descriptions"

https://www.hl7.org/fhir/device-definitions.html

[IHE-PCD-TF-G] IHE Technical Frameworks Appendix D: Glossary

http://ihe.net/uploadedFiles/Documents/Templates/IHE_TF_GenIntro_AppD_Glossary_Rev1.0_2014-07-01.pdf

[IEEE-11073] CEN ISO/IEEE 11073 Health informatics - Medical / health device communication standards

https://standards.ieee.org/downloads.html

[NIST-SP] NIST Special Publications

https://csrc.nist.gov/publications/sp

2.2 Reference Acquisition

- Center for Medical Interoperability, 8 City Boulevard, Suite 203, Nashville, TN 37209; Phone +1-615-257-6410; http://medicalinteroperability.org/
- Health Level Seven International (HL7), 3300 Washtenaw Avenue, Suite 227, Ann Arbor, MI 48104,US; Phone: +1 (734) 677-7777; http://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/
- Institute of Electrical and Electronics Engineers (IEEE), 3 Park Avenue, 17th Floor, New York, NY 10016-5997; http://www.ieee.org/

3 Terms and Definitions

This document relies on the terms and definitions specified in Section 5 of this document.

4 Abbreviations and Acronyms

This specification uses the following abbreviations:

API	Application Programming Interface
CMI	Center For Medical Interoperability
CNSSI	Committee on National Security Systems Instruction
FHIR	Fast Healthcare Interoperability Resources
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
IHE PCD	Integrating the Healthcare Enterprise Patient Care Device
ISO/IEC	International Standards Organization/International Electrotechnical Commision
NIST	National Institute of Standards and Technology
RFC	Request for Comments
SP	Special Publication
TD	Technical Document
U.S.C.	United States Code

5 Overview

This document is the result of reviews involving a number of existing standards to leverage existing “Terms and Definitions” and, of those, which are (a) the most suitable for The Center’s purposes; (b) have the best coverage for the relevant domain at hand; (c) are current and active. The conclusion was to use the following order for providing a definition for a Term or Definition:

Table 1 Priority of Terms and Definitions References

Prioritization Hierarchy	**Reference**
FHIR	[FHIR TD]
IEEE	[IEEE 11073]
IHE	[IHE-PCD TFG]
The Center	This document

In addition, security-related terms used in CMI documents are taken from [NIST SP]. The summary of the specified terms and definitions are below, in Table 2. Note that the second column in Table 2. provides references to the original source, when they exist. If no references are provided, then the definition was created by use within The Center’s efforts.

Table 2 Terms and Definitions

Term	References	Definition	Notes and examples	Category
Accumulation		A Gateway Device function that involves persisting all or a subset of the data it receives or acquires, and makes the persisted data available for queries.		Device or Client Interoperability Attributes
Aggregation		A Gateway Device function that involves receiving data from one or more Devices.		Device or Client Interoperability Attributes
Aggregator		A computer system that performs aggregation of data from source medical devices. An Aggregator is typically delivered as an appliance, serves one bedside, forwards data to a Gateway or Platform. Bernoulli, Capsule/Qualcomm, etc provide aggregators.		Device, Gateway Terms
Alerts		A warning or notification delivered to a user asynchronously to call the user's attention to an important or urgent clinical or equipment situation.		Computing Terms
ASUM Management Entity		A logical network element that implements the non-client portion of the ASUM interface as described in this document.		Device, Gateway Terms
Audit (Noun)		The result of Auditing.		Security and Certificates
Audit (Verb)	NIST SP 800-32	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.		Security and Certificates
Authenticate	NIST SP 800-32	To confirm the identity of an entity when that identity is presented.		Security and Certificates

Term	References	Definition	Notes and examples	Category
Authentication	NIST SP 800-53; SP 800-53A; SP 800-27; FIPS 200; SP 800-30	Verifying the identity of a user, process, or Device, often as a prerequisite to allowing access to resources in an information system.	For example for user authentication, this is typically accomplished by having the user provide credentials or authentication factors. For a Device or Gateway, this is typically accomplished using a signed certificate.	Security and Certificates
Authorization		Granting access to a resource or asset (such as a Device, application, process, or data) usually after authentication and according to a policy.		Security and Certificates
Availability	NIST SP 800-53; SP 800-53A; SP 800-18; SP 800-27; SP 800-37; SP 800-60; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542	Principle that authorized subjects are granted timely access to objects with sufficient bandwidth to perform the desired interaction.		Security and Certificates
Cache-And-Transfer		To Cache means to queue or accumulate data in such a way as to preserve its proper sequence. Cache-And-Transfer means the ability to Cache data when it cannot be transferred, and to transfer it once the ability to transfer is restored, in proper sequence.		Computing Terms

Term	References	Definition	Notes and examples	Category
Can be controlled via interface		The interface support sending data to the Device which modifies its state.	IV pump's rate might be changed, Ventilator's settings might be changed	Device or Client Interoperability Attributes
Can be queried for historical data		The Device accumulates data which can be queried through the interface.	A PACS system	Device or Client Interoperability Attributes
Care Team Member		A clinician or caregiver who is part of the team of persons caring for a patient. For example the patient's doctor and nurse are members of the patient's care team.		Clinical Informatics Terms
Certificate	NIST SP 800-32	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Validity Period, contains a Certificate serial number, and is digitally signed by the CA that issued the certificate.		Security and Certificates
Certificate Policy (CP)	CNSSI-4009; NIST SP 800-32	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision.		Security and Certificates

Term	References	Definition	Notes and examples	Category
Certificate Revocation List (CRL)		A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.		Security and Certificates
Certificate Signing Request (CSR)		A message conveying a request to have a Certificate issued.		Security and Certificates
Certification Authority (CA)		An entity authorized to issue, manage, revoke, and renew Certificates in the PKI.		Security and Certificates
Client		Generic term that can refer to either a Device or a Gateway that communicates with a Platform.		Device, Gateway, Platform Terms
Clinician Controlled		The Device can be activated or set by a clinician.	A ventilator is clinician controlled. A Patient Controlled Analgesia pump is clinician controlled.	Device Functional Attributes

Term	References	Definition	Notes and examples	Category
Confidentiality	NIST SP 800-53; SP 800-53A; SP 800-18; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.		Security and Certificates
Configuration		The ability to alter, or the manner by which is altered, the behavior of a Device, Gateway, or Platform without modifying its software. Configuration can be performed via a user interface, configuration files, or other similar approach.		Computing Terms
Connected Component		Any system that connects using one or more CMI specified interfaces.		Types of Devices
Connects to the patient		The Device touches the patient continuously or intermittently in order to perform its function.		Device Functional Attributes
Cryptographic		Methods, tools, and techniques pertaining to Cryptography.		Security and Certificates
Cryptography	NIST SP 800-59	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.		Security and Certificates

Term	References	Definition	Notes and examples	Category
Data Integrity	NIST SP 800-27	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.		Security and Certificates
Data Source		A Device or Gateway which provides clinical data to another Device, Gateway, or Platform.		Computing Terms
Device	[FHIR TD]	An instance or a type of a manufactured item that is used in the provision of healthcare without being substantially changed through that activity. The Device may be a medical or non-medical device. In CMI documents, the word Device usually refers to an Interoperable Medical Device as defined herein. Devices can be delivered as either software-only or a combination of software and hardware.		Device, Gateway Terms
Device Certificate		An end-entity non-CA certificate of the PKI chain installed in CMI Devices such as SAS Provider, Domain Proxy, Installer, PAL and CBSD Devices.		Security and Certificates
Diagnostic		A Device which is used to gather information to form a diagnosis and can transmit Text, Image, Video, raw waveform, and/or structured data.	Pulmonary Function, GI Endoscopy, ENT endoscopy, Vestibular Function, EKG, Evoked Response, Plethysmograph, Trans-esophageal Echo, etc…	Types of Devices
Digital Signature	NIST SP 800-63	An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.		Security and Certificates

Term	References	Definition	Notes and examples	Category
Elliptic Curve Cryptography (ECC)		A public-key cryptography system based on the algebraic structure of elliptic curves over finite fields.		Security and Certificates
Encryption		The process of changing plaintext into ciphertext through use of an encryption algorithm to provide security and privacy.		Security and Certificates
Encryption Algorithm	CNSSI-4009	Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.		Security and Certificates
Extensible Authentication Protocol (EAP)	IETF RFC 3748	An authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.		Security and Certificates
Forwarding		A Gateway Device function that involves routing, filtering, and/or forwarding data from one or more other Devices.		Device or Client Interoperability Attributes
Gateway		A Gateway is a computer system delivered as either a software application or hardware appliance which connects one or more Devices to another machine, application or Gateway. A Gateway typically provides one or more of the following functions: Aggregation, Forwarding, Translation, Accumulation. A Gateway typically serves multiple bedsides, typically forwards data to a Platform (Such as a CMI Platform) or a clinical IT application such as an EMR. A Gateway is typically provided by a device vendor to support that vendor's proprietary protocols (e.g. Draeger, Philips, GE, B Braun, etc. provide gateways).		Device, Gateway Terms

Term	References	Definition	Notes and examples	Category
Harm	ISO/IEC 51:1999, definition 3.3	Physical injury or damage to the health of people, or damage to property or the environment.		Security and Certificates
Has a digital interface		The Device has an interface and the data exchanged is digital (as opposed to analog).		Device or Client Interoperability Attributes
Has an Interface		The Device can exchange information to and/or from another Device.	Wired Networking interface, wireless networking interface, serial (RS-232, RS-422), parallel (IEEE 1284), USB, Bluetooth 2, Bluetooth 4, etc	Device or Client Interoperability Attributes
Has network capability		The Device has Bluetooth, WiFi, Ethernet, or other TCP/IP network protocol support.		Device or Client Interoperability Attributes
Hash		The output of a Hash Function.		Security and Certificates
Hash Function	NIST SP 800-63, FIPS 201	A function that maps a bit string of arbitrary length to a fixed length bit string. Robust hash functions satisfy the following properties: 1) One-Way. It is computationally infeasible to find any input that maps to any prespecified output. 2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.		Security and Certificates
Health System Certificate		A Digital Certificate used for a Health System,		Security and Certificates
Hybrid		A Device that is a combination of other Devices.		Types of Devices

Term	References	Definition	Notes and examples	Category
Identity		The set of characteristics, including PKI certificates, network addresses, and user accounts (user ID and password) by which an individual, Device or Gateway is uniquely recognizable.		Security and Certificates
Imaging		A Device that captures images and/or archives and/or communicates images.	A PACS system, a medical wound imaging system	Types of Devices
Integrity		The property that information, Devices, or communications have not been improperly modified or destroyed, including ensuring information non-repudiation and authenticity.	This definition extends on scope included in NIST to include all aspects of interest to CMI.	Security and Certificates
Interoperable Device		A Device which has the capability of electronically transmitting or receiving commands, measurements, settings, alarms, or any other type of information. An Interoperable Device can also meet the definition of a Gateway if it has Gateway functionality.		Device, Gateway, Platform Terms
Locating		A Device that captures geographic location	An RTLS device for tracking providers, equipment, or patients	Types of Devices
Managed Digital Certificates Authority		An entity which controls and secures the assignment and revocation of Digital Certificates.		Security and Certificates
Mapping		A Gateway or Device function that involves mapping data it receives or acquires from one distinct data model into another.		Device or Client Interoperability Attributes

Term	References	Definition	Notes and examples	Category
Medical Device	[FHIR TD]	Medical Devices include durable (reusable) medical equipment, implantable devices, as well as disposable equipment used for diagnostic, treatment, and research for healthcare and public health. Unless the phrase “Non-medical Device” is used, the term “Device” can generally be understood as “Medical Device” in The Center’s documents.		Device, Gateway Terms
Medical Interoperability Platform, or Platform		A computer system that complies with the Center's clinical data interoperability interface requirements to communicate with clients. It may also have other elements, such as data stores and APIs for applications such as electronic medical record systems, clinical decision support systems etc.		Device, Gateway Terms
Message Integrity		Verification that received messages between communicating parties are authentic, that is what was sent by the sender is what is received by the recipient. Often achieved using a message authentication code (MAC).		Security and Certificates
Modular		A Device that has optional modules.		Types of Devices
Monitoring		Synchronous acquisition of Vitals and other measurements.		Clinical Informatics Terms
Monitoring		A Device, including Primitive Devices, which acquires information from a patient and transmits this either continuously or intermittently.	ICU monitor, EEG monitor, Smart Bed, Capnography, Cardiac Output	Types of Devices
Non-medical Device	[FHIR TD]	Non-medical Devices include items such as a machine, cellphone, computer, application, printer etc.		Device, Gateway Terms

Term	References	Definition	Notes and examples	Category
Non-repudiation	CNSSI-4009 and NIST SP 800-60	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.		Security and Certificates
Not interoperable		The Device is not an Interoperable Device.	An electronic cuff pressure machine used at home that doesn't have an interface capability	Device or Client Interoperability Attributes
Notification		An asynchronous message or alert conveying an error or other unexpected condition.		Computing Terms
Patient aware		The Device holds a patient identifier		Device Functional Attributes
Patient Controlled		The Device can be activated or set by a patient.	A home health scale is patient controlled. A Patient Controlled Analgesia pump is patient controlled.	Device Functional Attributes
Personal Health Device		A Device that is owned or maintained by the patient, including a scale, blood pressure measurement Device, a glucometer, an activity monitor, etc.		Device, Gateway Terms
PKI Trust Anchor	NIST SP 800-57 Part 1	A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates.		Security and Certificates
Platform Service		A collective term for connected components that implement functionalities supporting trust and data liquidity, as specified and enabled by CMI's Trusted Platform model.		Device, Gateway, Platform

Term	References	Definition	Notes and examples	Category
Point Of Care Device		A Device used in a patient care setting such as a hospital, clinic or, if not owned or maintained by the patient, in the home.		Device, Gateway Terms
Primitive		An interoperable Device which is merely capable of transmitting an unsolicited data packet every few seconds/minutes.	Simple pulse oximetry or non-invasive blood pressure device	Types of Devices
Privacy		Ensuring access to communications or data is restricted only to authorized parties in accordance with federal laws and institutional (such as a care provider) policies.		Security and Certificates
Private Key	NIST SP 800-57 Part 1	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to: 1) Compute the corresponding public key, 2) Compute a digital signature that may be verified by the corresponding public key, 3) Decrypt keys that were encrypted by the public key, or 4) Compute a shared secret during a key-agreement transaction.		Security and Certificates
Provision		To configure or otherwise set up a Device or Gateway so that it can be handed off to an end-user and/or made ready for use.		Computing Terms

Term	References	Definition	Notes and examples	Category
Public Key	NIST SP 800-57 Part 1	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone.		Security and Certificates
Public Key Infrastructure (PKI)		The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.		Security and Certificates
Receive-only		The Device can only receive, but cannot send clinical data[1].		Device or Client Interoperability Attributes
Resource		A physical or virtual asset that can be used to perform a function.		Computing Terms
RSA		A public key cryptographic system (algorithm) invented by Rivest, Shamir, and Adelman.		Security and Certificates
Secure Connection		A type of Device or Gateway connection which has enabled certain minimum security attributes such as encryption and authentication.		Security and Certificates

[1] Clinical data as opposed to data that might be necessary as part of the device protocol. For example, an “ack”(acknowledgement) in response to the device transmitting clinical data is not clinical data

Term	References	Definition	Notes and examples	Category
Secure Software Download		A mechanism used to safely deploy new software to a managed Device and attest the authenticity of the Software. Safely in this context means that the downloaded Software is cryptographically signed and attestable by the Device being updated.		Security and Certificates
Secure Software Update		A mechanism used to securely determine if a managed Device's Software needs to be updated, the subsequent secure Software download if an update is required, and the further subsequent safe execution of the downloaded Software.		Security and Certificates
Secure Transport		The digital transport of data performed in a secure manner, to include encryption, endpoint authentication, and data integrity.		Security and Certificates
Security Log		A data set whose purpose is to aid in the analysis of a security breach or other abnormal or illegal event by providing evidence or clues relating to that event.		Security and Certificates
Sensor		A probe or other measurement Device that touches or is wearable on a patient's body includes some means to communicate the measurements	Home weight scale, glucose measurement patch, ECG wearable sensor	Types of Devices

Term	References	Definition	Notes and examples	Category
Service		A Service is a software module which consists of an interface, a contract, and an implementation, to achieve a particular computing task. There is a service provider and a service consumer. The interface defines how the provider will process the requests from the consumer, the contract defines the specific data and protocol interaction between the provider and consumer, and the implementation is the actual software code for the service.		Computing Terms
Service Discovery		The automatic detection of devices and the services they offer on a computer network. This is achieved through Service Discovery Network Protocol(s).		Computing Terms
Software		Firmware, drivers, operating system, and application program components necessary for a Device or Gateway to perform its intended functions.		Computing Terms
Software Repository		The logical network entity from which a client can obtain the software updates.		Computing Terms
Spot Check		Asynchronous acquisition of Vitals and other measurements.		Clinical Informatics Terms
Static		A Device that has no modularity		Types of Devices
Supports communication standard(s)		The Device communicates using one or more standards.	e.g. IHE PCD 01	Device or Client Interoperability Attributes
Supports nomenclature standard(s)		The Device identifies clinical concepts using one or more standards.	e.g. IEEE 11073.1001	Device or Client Interoperability Attributes

Term	References	Definition	Notes and examples	Category
Supports security standard(s)		The Device supports security related standards.	e.g. TLS, XAML, OAuth, Hotspot 2.0	Device or Client Interoperability Attributes
Therapeutic		A Device that delivers something into a patient's body such as fluids, medication, oxygen	Patient-Controlled analgesia pump, IV pump, Ventilator	Types of Devices
Threat	SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.		Security and Certificates
Threat source	NIST FIPS 200; SP 800-53; SP 800-53A; SP 800-37	Intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.		Security and Certificates
Transformation		A Gateway or Device that performs one or more of: Translation, Mapping, Filtering.		Device or Client Interoperability Attributes
Translation		A Gateway or Device function that involves translating data it receives or acquires from the form used by one system into the form required by another.		Device or Client Interoperability Attributes
Transmit/Receive		The Device can receive and send clinical data.		Device or Client Interoperability Attributes
Transmit-only		The Device can only send, but cannot receive clinical data.		Device or Client Interoperability Attributes

Term	References	Definition	Notes and examples	Category
Transmits Continuously		The Device transmits at least once per minute.	ICU monitor, telemetry	Device or Client Interoperability Attributes
Transmits Episodically		The Device transmits data irregularly, in a clinical event-based fashion.	an electronic fall monitor transmits data when it detects a potential fall	Device or Client Interoperability Attributes
Transmits Periodically		The Device transmits at most once per minute.	A non-invasive blood pressure device can be set for 5 minutes but not every minute	Device or Client Interoperability Attributes
Transport Layer Security (TLS)	IETF RFC 5246	Provides communication security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.		Security and Certificates
Trust		A decision to believe and rely on the identity of a Device or individual that becomes the foundation for all other security controls and activities.		Security and Certificates
Trust Anchor		A root of trust on which security decisions are made. In the context of the CMI, the Trust Anchor is the root certificate to which all other certificates chain.		Security and Certificates
Trusted Device		A Device for which Trust has been established.		Security and Certificates
Trusted Infrastructure		A computing infrastructure for which Trust has been established.		Security and Certificates
Trusted Wireless Health		Wireless data transmission infrastructure used for healthcare for which Trust has been established.		Security and Certificates

Term	References	Definition	Notes and examples	Category
User Aware		The Device has the notion of different users or user roles.		Device Functional Attributes
User Role Aware		The Device has the notion of user roles – for example a patient, clinician, biomedical engineer, administrator might be users.		Device Functional Attributes
Vendor Software Update Server		A logical network component that is part of the client manufacturer's network that can provide information related to software updates.		Device, Gateway Terms
Vitals		Clinical measurements meant to measure the body's vital or essential functions, including Heart Rate, Blood Pressure, Temperature, Oxygen Saturation, Respiration.		Clinical Informatics Terms
Vulnerability	NIST SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.		Security and Certificates
Waveform		The shape and form of a signal over time, usually sampled at more than 1 Hz. An electrocardiogram, a cardiorespirogram are examples of waveforms.		Clinical Informatics Terms
Wired interface		The interface is through a physical port on the Device	Serial/parallel port, Ethernet, USB, etc…	Device or Client Interoperability Attributes
Wireless interface		The interface is wireless.	WiFi, Bluetooth, etc…	Device or Client Interoperability Attributes

Term	References	Definition	Notes and examples	Category
Zero-touch protocols		Networking protocols used to achieve zero-touch provisioning, which allows the secure insertion of a Device onto a network without manual intervention.		Security and Certificates

6 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.

JF Lancelot authored the original version of this document. Special thanks to the following who were directly involved via a variety of discussions, reviews and input: **Paul Schluter, Ken Fuchs, Eldon Metz, Bowen Shaner, Stuart Hoggan, Sumanth Channabasappa** and, **Steve Goeringer** (security terms and definitions).

This work was conducted within the Center's Architecture & Requirements, Connectivity, and Security working groups, whose members have including the following part-time and full-time participants during the creation of this version of the document:

Working Group Participants	Company Affiliation
Aishwarya Muralidharan	vTitan
Alex Poiry	Cerner
Ali Nakoulima	Cerner
Andrew Meshkov	86Borders
Brian Long	Masimo
Brian Scriber	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
Guy Johnson	Zoll
Ian Sherlock	Texas Instruments
James Surine	Smiths-Medical

Working Group Participants	Company Affiliation
Jason Mortensen	Bernoulli Health
Jay White	Laird
Jay White	Laird
Jeffrey Brown	GE
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 PhD	CablelLabs
Mike Krajnak	GE
Milan Buncick	Aegis
Neil Puthuff	RTI
Neil Seidl	GE
Ponlakshmi G	vTitan
Scott Eaton	Mindray
Stefan Karl	Philips
Steven Goeringer	CableLabs
Travis West	Bridge Connector

- Sumanth Channabasappa (Chief Architect),, Steve Goeringer (Chief 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