CENTER *for* MEDICAL
INTEROPERABILITY

The Center for Medical Interoperability Specification Clinical Data Interoperability Based on IHE PCD – Identity and Secure Transport

CMI-SP-CDI-IHE-PCD-IST-D02-2019-05-31

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.

Table of Contents

Document Status Sheet

Document Control Number:	CMI-SP-CDI-IHE-PCD-IST
Document Title:	Clinical Data Interoperability Based on IHE PCD – Identity & Secure Transport
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 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.

1 Scope

1.1 Introduction and Purpose

This document presents non-data transmission requirements for clients that leverage Integrated Healthcare Enterprise (IHE) Patient Care Device (PCD) Health Level Seven (IHE PCD HL7) for clinical data transmission. It includes requirements for the clients to leverage the foundational requirements such as identities, provisioning flow, access network connectivity etc. It also specifies how traffic is secured using Transport Layer Security (TLS) with proven industry standard encryption and message authentication algorithms. These security features help protect against client spoofing, unauthorized access, information disclosure, and tampering.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"SHALL" This word means that the item is an absolute requirement of this specification.

"SHALL NOT" This phrase means that the item is an absolute prohibition of this specification.

"SHOULD" This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

"MAY" This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 References

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification.

Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

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

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

[IETF-RFC5289] TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

https://tools.ietf.org/html/rfc5289

[IETF-RFC5288] AES Galois Counter Mode (GCM) Cipher Suites for TLS

https://tools.ietf.org/html/rfc5288

[IETF-RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

https://tools.ietf.org/html/rfc5280

[IETF-RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

https://tools.ietf.org/html/rfc6960

[IETF-RFC6961] "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", IETF RFC, June 2013

https://tools.ietf.org/html/rfc6961

[FIPS-140-2] Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001.

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[CMI-SP-F-ID] Identity

https://medicalinteroperability.org/specifications

[CMI-SP-F-PF] Provisioning Flows

https://medicalinteroperability.org/specifications

[CMI-SP-F-ASUM] Automated Secure Update and Management Framework

https://medicalinteroperability.org/specifications

[CMI-SP-F-ASUM-MEM-DMC] ASUM Solution for IHE PCD Clients Using MEM DMC

https://medicalinteroperability.org/specifications

[CMI-SP-CDI-IHE-PCD-SSE] Clinical Data Interoperability Based on IHE PCD – Semantics, Syntax, and Encoding

https://medicalinteroperability.org/specifications

[IHE-PCD-MEM-DMC] Integrating the Healthcare Enterprise (IHE) Medical Equipment Management (MEM) Device Management Communication (DMC)

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

2.2 Informative References

This specification uses the following informative reference.

[CMI-DOC-TD] Terms and Definitions

https://medicalinteroperability.org/specifications

[CMI-TR-OVERVIEW] Foundational & Clinical Data Interoperability Efforts Overview

https://medicalinteroperability.org/specifications

[CMI-SP-F-CP] Certificate Policy

https://medicalinteroperability.org/specifications

2.3 Reference Acquisition

- Center for Medical Interoperability, 8 City Boulevard, Suite 203 | Nashville, TN 37209; Phone +1-615-257-6410; https://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, https://www.ietf.org
- The Institute of Electrical and Electronics Engineers, Inc., 3 Park Avenue, New York, NY 10016-5997, USA Phone: +1-732-981-0060, Fax: +1-732-562-1571, http://standards.ieee.org/findstds/index.html

3 Terms and Definitions

This specification uses the terms and definitions in [CMI-DOC-TD]

4 Abbreviations and Acronyms

This specification uses the following abbreviations:

AES	Advanced Encryption Standard
ASUM	Automated Secure Update Mechanism
CMI	Center For Medical Interoperability
CRL	Certificate Revocation List
DHE	Diffie-Hellman Exchange
DOC	Device Object Consumer
DOR	Device Object Reporter
ECC	Elliptic curve
ECDHE	Elliptic curve Diffie-Hellman key exchange
EHR	Electronic Health Record
HL7	Health Level Seven International
IHE PCD	Integrating the Healthcare Enterprise Patient Care Device
MLLP	Minimum Lower Layer Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RSA	Rivest–Shamir–Adleman
TLS	Transport Layer Security

5 Overview

For an overview of the CMI architecture, and a separation of the foundational and clinical data interoperability efforts, please refer to [CMI-TR-OVERVIEW]. This document is part of the clinical data interoperability efforts and focuses on clients that support IHE PCD for clinical data interoperability, client management and automated secure update mechanism (ASUM). It specifies how such clients can leverage the foundational efforts and extensions to secure the transport layer.

Within the CMI architecture medical devices and gateways are collectively referred to as clients (see: [CMI-DOC-TD]. The Current scope of the efforts focus on interfaces between clients and other connected components, such as platform service components. The CMI foundational document set (see: [CMI-TR-OVERVIEW]) specify the non-clinical data interfaces. These include a provisioning flow that incorporates how a client connects to a wired or wireless access network, obtains basic configuration (e.g., time server, service discovery parameters), discovers a client management entity to request authorization, and connects to platform services for clinical data communications. It also allows for the client to be directed for secure software update as required. For more information, please refer to [CMI-SP-F-PF]. For automated and secure update mechanism (ASUM), see [CMI-SP-F-ASUM]. For ASUM solution for clients supporting IHE PCD, see [CMI-SP-F-ASUM-MEM-DMC]. Further, the client will leverage the Identity and profile requirements specified in [CMI-SP-F-ID]. This document specifies how these foundational documents are leveraged for secure data interoperability. Further, for clients that support Minimum Lower Layer Protocol (MLLP) for transport, this document provides security requirements by utilizing TLS requirements specified in [CMI-SP-F-PF].

6 Requirements for Connected Components That Support IHE PCD

This section outlines requirements for clients and platform services that support IHE PCD. It relies on requirements in foundational and other clinical data interoperability specifications.

6.1 Client Provisioning Flow

Clients that implement IHE PCD SHALL support the client provisioning flow, resiliency and management requirements as specified in [CMI-SP-F-PF].

6.2 Identity and Secure Transport Requirements

This section specifies implementation requirements for connected components to establish a secure TLS connection for IHE PCD HL7 messaging using MLLP. It is a assumed that the client has obtained network access. A certificate (issued by the CMI PKI) is used for mutual authentication of platform services and Clients. Certificate hierarchy and profile details are defined in [CMI-SP-F-CP]. Medical device manufacturers and hospital members contact The Center to register and acquire digital certificates. This specification assumes equivalent functional behaviors from clients whether implemented on medical devices and gateways relative to implementation of secure transport for IHE PCD.

The following requirements rely on the following foundational specifications: [CMI-SP-F-ID] and [CMI-SP-F-PF].

- Clients SHALL comply with the identity requirements as specified in [CMI-SP-F-ID]
- Clients SHALL use TLS, specifically Interface B requirements as specified in [CMI-SP-F-PF], Annex B for clinical data communications
- Clients SHALL use TLS, specifically Interface B requirements as specified in [CMI-SP-F-PF], Annex B for client management communications
- Platform services for clinical data communications SHALL comply with the identity requirements as specified in [CMI-SP-F-ID].
- Platform services for clinical data communications with clients SHALL support TLS, specifically Interface A requirements as specified in [CMI-SP-F-PF], Annex B.
- Client management entity SHALL comply with the identity requirements as specified in [CMI-SP-F-ID].
- Client management entity SHALL support TLS, specifically Interface A requirements as specified in [CMI-SP-F-PF], Annex B.
- ASUM management entity SHALL comply with the identity requirements as specified in [CMI-SP-F-ID].
- ASUM management entity SHALL support TLS, specifically Interface A requirements as specified in [CMI-SP-F-PF], Annex B.

6.3 Client Management Requirements

Clients SHALL support the client management requirements as specified in [CMI-SP-F-PF]. Clients SHALL also support the applicable client to client management entity requirements specified in Annex A of this document.

Client management entities SHALL also support the applicable client management requirements as specified in [CMI-SP-F-PF]. Client management entities SHALL also support the applicable client to client management entity requirements specified in Annex A of this document.

6.4 ASUM Requirements

Clients SHALL support the ASUM requirements as specified in [CMI-SP-F-ASUM] and [CMI-SP-F-ASUM-MEM-DMC].

ASUM management entities SHALL support the applicable requirements as specified in [CMI-SP-F-ASUM] and [CMI-SP-F-ASUM-MEM-DMC].

6.5 Clinical Data Transmission Requirements

Clients supporting IHE PCD SHALL support the clinical data requirements specified in [CMI-SP-CDI-IHE-PCD-SSE].

6.6 Additional Resiliency Considerations

Implementations should consider a network failure between Device Observation Reporter (DOR) to Device Observation Consumer (DOC) or off-line condition of the (DOC). In this case the DOR recognizes a network failure based on one or more indications of failure, including, but not limited to (1) failure to receive a timely HL7 V2 MLLP ack or (2) receives some other indication from the DOC, the network infrastructure, or other entity indicating that communication is not possible, or other indication that the DOR (e.g. CIC/HIS/EMR) system has gone 'off-line'. In this case, the DOR SHOULD 'store-and-forward' the outbound messages for a user configurable period of time (e.g. 12 hours) and transmit the information once network communication and DOR availability has been re-established. [Although messages that stored and forwarded at a later time may not provide 'near real-time information' the delayed information is still useful as part of the patient record and quality assurance on information that was manually recorded while the network and/or DOR was unavailable.]

7 Annex A: Client to Client Management Entity Requirements

Client to Client Management Entity (CME) communication leverages [IHE-PCD-MEM-DMC] to establish Client communications and exchange Minimum Connected Component Profiles (MCCP). The [IHE-PCD-MEM-DMC] PCD-15 message containing an MCCP is sent periodically from the Client to the CME. The CME then acknowledges the message with its own MCCP.

After basic communication is established, the CME determines whether a Client's software needs to be updated before proceeding. If so, the CME directs the Client to communicate with the ASUM Management Entity [CMI-SP-F-ASUM-MEM-DMC].

7.1 Periodic PCD-15 Message with MCCP

Clients SHALL periodically send a [IHE-PCD-MEM-DMC] PCD-15 message to the Client Management Entity (CME) containing the Minimum Connected Component Profile (MCCP). Clients SHALL use a default periodicity of five minutes. Clients SHALL allow for this default to be modified to meet deployment requirements. Clients SHALL use the following message structure for the MCCP:

- OBX-3 contains 126976^MDCC4MI_ATTR_CMI_MCCP^MDC
- OBX-5 contains the MCCP

7.2 CME Acknowledgement with MCCP

The CME SHALL acknowledge all PCD-15 messages containing MCCPs using the HL7 ACK, with their own MCCP included in an informational error segment. The CME SHALL use the following message structure for the acknowledgement:

- ERR-5 contains 126976^MDCC4MI_ATTR_CMI_MCCP^MDC
- ERR-7 contains the MCCP as specified in section 3

7.3 MCCP Format Negotiation

The Client and CME SHALL follow the MCCP format negotiation steps outlined in CMI-SP-F-ID. If the CME does not support the Client's MCCP format version, the CME SHALL respond with a list of its supported MCCP versions in a separate ERR segment in the ACK using the following message structure:

- ERR-5 contains 126977^MDCC4MI_ATTR_CMI_MCCP_LIST^MDC
- ERR-7 contains the list of supported MCCP versions, separated by spaces

7.4 CME Response to Initial Communication

In response to an initial communication from a Client, the CME SHALL include an authorized/deauthorized indication and FQDNs for the ASUM management entity and Clinical Data Exchange, if authorized, using the following message structure:

- ERR-5 contains 126978^MDCC4MI_ATTR_CMI_CME_RESPONSE^MDC
- ERR-7 contains keyvalue pairs separated by spaces, defined in Table 2.

Table 1

Key	Description	Example
AUTH_STATUS	Authorization status	AUTH_STATUS=AUTHORIZED
ASUM_HOST	FQDN of the ASUM Management Entity	ASUM_HOST=asum.some_hospital.com
ASUM_PORT	ASUM Management Entity port	ASUM_PORT=2575
CDE_HOST	FQDN of the Clinical Data Exchange	CDE_HOST=cde.some_hospital.com
CDE_PORT	Clinical Data Exchange port	CDE_PORT=2575

7.5 CME Configure Periodicity Command

If the periodicity of a Client's PCD-15 message is to be configured, the CME SHALL send the command using a separate ERR segment in the ACK. The CME SHALL use the following message structure:

- ERR-5 contains 126981^MDCC4MI_ATTR_CMI_CME_CMD^MDC
- ERR-6 contains the unique identifier for the command
- ERR-7 contains CMD=CFG_INTERVAL with the parameter in Table 2.

Table 2

Key	Description	Example
INTERVAL	Periodicity of PCD-15, in seconds	INTERVAL=300

In response to the CFG_INTERVAL command, the Client SHALL perform the reconfiguration of the interval as requested. Clients SHALL indicate success or failure to the CME after processing the Configure Interval command in the first PCD-15 message after the configuration change was attempted using the corresponding management codes in CMI-SP-F-ASUM. The Client SHALL continue to indicate success or failure of configuration command to the CME until a successful ACK is received.

7.6 Message Structure

CME and Client acknowledgements SHALL adhere to the following restrictions beyond normal HL7 restrictions on ERR-7:

Keys cannot contain '=' char

Values cannot contain '=' char unless it is escaped as %3D
Values cannot contain ' ' char unless it is escaped as %20

Note that ERR-7 has a maximum length of 2048.

7.7 MCCP Structure

MCCPs communicated via PCD-15 or ACK messages SHALL use the key-value pairs defined in Table 3, separated by spaces. The values in each key-value pair SHALL follow the structure defined in [CMI-SP-F-ID].

Table 3 - MCCP Key-Value Pairs

Key	Description	Example
MCCP_VER	Minimum Connected Component Profile Format Version	MCCP_VER=001
CCID	Connected Component Identifier	CCID=[Version]:[VendorID]:[Type]:[ComponentID]
RBV	Release Bundle Version	RBV=1.0.0
CCS	Current Component Status	CCS=Operational
SWV	Software Version	SWV=1.0.0
MM	Make and Model	MM=CMI 4000
FCCP	Full Connected Component Profile URI	FCCP =https://medicalinteroperability.org/make_model_xyz
CONFIG	Connected Component Configuration Data URI	CONFIG = https://medicalinteroperability.org/make_model_xyz/config
OPT	Optional Information	OPT=Additional Information

The notation is described below in simplified BNF:

```
<syntax>       ::= <MCCP_VER> <parameters>

<mccp_ver>     ::= "MCCP_VER"= 001 - 999

<parameters>   ::= <parameter> | <parameters>
```

```
<parameter>   ::= <key> “=” <value>

<key>         ::= text

<value>       ::= text
```

7.8 Example Messages (Informative)

This section provides examples of PCD-15 messages with MCCPs.

7.8.1 Sample PCD-15 Message with MCCP

```
MSH|^~\&|CMI^001A010000000001^EUI-64||CMI HOSPITAL||20150119221713-
0000||ORU^R01^ORU_R01|1421727433|P|2.6|||AL|NE||UNICODE UTF-
8|en^English^ISO639||IHE_PCD_015^IHE
PCD^1.3.6.1.4.1.19376.1.6.1.15.1^ISO
PID|1||||||||||||||||||||||||||||||Y
PV1|1|N
OBR|1|2000101^CMI 4000^001A010000000001^EUI-64|2000101^CMI
4000^001A010000000001^EUI-
64|126979^MDCC4MI_EVT_CMI_DEVICE_INFO^MDC|||20150119221713-0000
OBX|1|ST|126976^MDCC4MI_ATTR_CMI_MCCP^MDC|1.0.0.1|MCCP_VER=001
CCID=01:CMI:HOST:4000 RBV=1.0.0 CCS=Operational SWV=1.0.0
MM=CMI%204000 FCCP=https://medicalinteroperability.org/make_model_xyz
CONFIG=https://medicalinteroperability.org/make_model_xyz/config
OPT=Additional%20Info||||||X
```

7.8.2 Sample ACK with MCCP

```
MSH|^~\&|MgmtEntityABC||VendorXYZ ^001A010000000001^EUI-
64||20150119221714-0000||ACK^015^ACK|1421727433|P|2.6|||NE|NE||UNICODE
UTF-8|en^English^ISO639||IHE_PCD_015^IHE
PCD^1.3.6.1.4.1.19376.1.6.1.15.1^ISO
MSA|AA|1421727433
ERR||0^Message
Accepted^HL70357|I|126976^MDCC4MI_ATTR_CMI_MCCP^MDC||MCCP_VER=001
CCID=[Version]:[VendorID]:[Type]:[ComponentID] RBV=1.0.0
CCS=Operational SWV=1.0.0 MM=CMI%204000
FCCP=https://medicalinteroperability.org/make_model_xyz
CONFIG=https://medicalinteroperability.org/make_model_xyz/config
OPT=Additional%20Info
```

7.8.3 Sample ACK with Supported MCCP List

```
MSH|^~\&|MgmtEntityABC||VendorXYZ ^001A010000000001^EUI-
64||20150119221714-0000||ACK^015^ACK|1421727433|P|2.6|||NE|NE||UNICODE
UTF-8|en^English^ISO639||IHE_PCD_015^IHE
PCD^1.3.6.1.4.1.19376.1.6.1.15.1^ISO MSA|AA|1421727433
ERR||0^Message
Accepted^HL70357|I|126977^MDCC4MI_ATTR_CMI_MCCP_LIST^MDC||001 002 003
```

7.8.4 Sample ACK with MCCP and CME Response

```
MSH|^~\&|MgmtEntityABC||VendorXYZ ^001A010000000001^EUI-
64||20150119221714-0000||ACK^015^ACK|1421727433|P|2.6|||NE|NE||UNICODE
UTF-8|en^English^ISO639||IHE_PCD_015^IHE
PCD^1.3.6.1.4.1.19376.1.6.1.15.1^ISO
MSA|AA|1421727433
ERR||0^Message
Accepted^HL70357|I|126976^MDCC4MI_ATTR_CMI_MCCP^MDC||MCCP_VER=001
CCID=[Version]:[VendorID]:[Type]:[ComponentID] RBV=1.0.0
CCS=Operational SWV=1.0.0 MM=CMI%204000
FCCP=https://medicalinteroperability.org/make_model_xyz
CONFIG=https://medicalinteroperability.org/make_model_xyz/config
OPT=Additional%20Info
ERR||0^Message
Accepted^HL70357|I|126978^MDCC4MI_ATTR_CMI_CME_RESPONSE^MDC||AUTH_STAT
US=AUTHORIZED ASUM_HOST=asum.some_hospital.com ASUM_PORT=2575
CDE_HOST=cde.some_hospital.com CDE_PORT=2575
```

7.8.5 Sample ACK with MCCP and Configure Periodicity Command

```
MSH|^~\&|MgmtEntityABC||VendorXYZ ^001A010000000001^EUI-
64||20150119221714-0000||ACK^015^ACK|1421727433|P|2.6|||NE|NE||UNICODE
UTF-8|en^English^ISO639||IHE_PCD_015^IHE
PCD^1.3.6.1.4.1.19376.1.6.1.15.1^ISO
MSA|AA|1421727433
ERR||0^Message
Accepted^HL70357|I|126976^MDCC4MI_ATTR_CMI_MCCP^MDC||MCCP_VER=001
CCID=[Version]:[VendorID]:[Type]:[ComponentID] RBV=1.0.0
CCS=Operational SWV=1.0.0 MM=CMI%204000
FCCP=https://medicalinteroperability.org/make_model_xyz
CONFIG=https://medicalinteroperability.org/make_model_xyz/config
OPT=Additional%20Info
ERR||0^Message
Accepted^HL70357|I|126981^MDCC4MI_ATTR_CMI_CME_CMD^MDC|123456|CMD=CFG_
INTERVAL INTERVAL=300
```

8 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.

Stuart Hoggan authored the original version of this document, with edits by **Steve Goeringer**. Special thanks to the following who were directly involved via a variety of discussions, reviews and input for the D01 version: **Ken Fuchs, JF Lancelot, Kai Hassing** and **Paul Schluter**.

This version of the document (D02) contains structural changes to move certain requirements (such as TLS) to the foundational efforts that are now referenced here. These were authored by **Sumanth Channabasappa.** It also adds requirements for MEM DMC communications, which were

authored by **Jacob Chadwell**. Finally, the additional resiliency considerations were authored by **Paul Schluter.**

This effort was conducted within the Center's Architecture and Requirements and Security working groups, 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
Ali Nakoulima	Cerner
Andrew Dobbing	Laird
Barry Brown	Mortara
Bill Hagestad	Smiths Medical
Bill Pelletier	GE
Bo Dagnall	HPE
Bruce Friedman	GE Healthcare
Corey Spears	Infor
Damon Herbst	Cerner
Doug Bogia	Intel
Doug Smith	Laird
Eldon Metz	Innovision Medical
Erik Eckman	Microsoft
Guy Johnson	Zoll
Jay White	Laird
Jeff Brown	GE
JF Lancelot	Airstrip
John Zaleski	Bernoulli Health
Dr. Jorg-Uwe Meyer	MT2IT
Kai Hassing	Philips
Ken Fuchs	Draeger

WG Participant	**Company Affiliation**
Kurt Elliason	Smiths Medical
Dr. Max Pala	CableLabs
Peter Housel	Masimo
Scott Eaton	Mindray
Song Chung	Welch Allyn
Soundharya Nagasubramanian	Welch Allyn
Stefan Karl	Philips
Stuart Hoggan	CableLabs

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