Integrating the Healthcare Enterprise

IHE Patient Care Coordination Technical Framework Supplement

Remote Patient Monitoring (RPM)

Rev. 2.0 – Draft for Public Comment

Date: May 26, 2017

Author: PCC Technical Committee

Email: pcc@ihe.net

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Foreword

This is a supplement to the IHE Patient Care Coordination Technical Framework V11.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on May 26, 2017 for public comment. Comments are invited and may be submitted at http://www.ihe.net/PCC_Public_Comments. In order to be considered in development of the trial implementation version of the supplement, comments must be received by June 25, 2017.

This supplement describes changes to the existing technical framework documents.

"Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume.

Amend Section X.X by the following:

Where the amendment adds text, make the added text **bold underline**. Where the amendment removes text, make the removed text **~~bold strikethrough~~**. When entire new sections are added, introduce with editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

General information about IHE can be found at http://ihe.net.

Information about the IHE Patient Care Coordination domain can be found at http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE Patient Care Coordination Technical Framework can be found at http://ihe.net/Technical_Frameworks.

CONTENTS

Introduction to this Supplement

This supplement describes a standardized means of reporting measurements taken by Personal Healthcare devices in a remote location whereby remote it means outside of the healthcare provider facilities and is typically the patient's home, and reporting those measurements to the health care provider.

Open Issues and Questions

How to specify the FHIR®[1] transactions? PCHA cannot get this specification done fast enough. Certain European nations are already implementing this profile in the proposed extension where FHIR replaces the PHMR.

There are two FHIR transactions. The first is where a FHIR Bundle replaces the PCD-01 message in the hData upload. The FHIR Bundle contains all the information of the PCD-01 message but using the FHIR data model. It is expected to be an additional 'Communicate Data' transaction. The second is where the Content Module generates content for consumption using the FHIR data model. RESTful FHIR transactions are used to place the data on a RESTful FHIR server for consumption by a Content Consumer. It is not clear how to specify this option but it is currently the driving use case for the RPM.

Is it reasonable to support a model where the DeviceObservationConsumer is grouped with a Content Consumer?

Should we add a third Content Creator that provides the PCD-01 V2 message? There seems to be support for this feature in PCD.

Transaction numbering. A lot of the transaction numberings are wrong. Here are the correct numbers listed on the PCC wiki

- Communicate PCHA Data Transaction (RPM) [PCC-15]
- Communicate PCD Data-hData (RPM) [PCC-21]
- Communicate PCD Data-SOAP (RPM) [PCC-22]
- Communicate FHIR Data-hData (RPM) [PCC-42]
- Share FHIR Resources (RPM) [PCC-43]

Closed Issues

6. Comments from Paul Schluter - A few suggestions:

[1] FHIR is the registered trademark of Health Level Seven International.

1. Indicate that several deployment options are shown, in each of the three horizontal bands. A short description of each as a subcaption in small italic text would help the reader understand what is going on.
2. PCD DOR and PCD DOC are defined by the IHE PCD domain. You need a unique label for your device data observation source and consumer; it should not be the same as those that have been used by IHE PCD for years.
3. Use shaded vertical lines to highlight that the PCHA data transaction(s), IHE PCD DEC (of which we have many, in addition to the basic PCD-01), and PCC document sharing.

Response to Issue 6: The suggestions from Paul Schluter have been taken into consideration with modification by committee. Some of the diagrams were put in landscape mode instead of vertical to make the flow easier to visualize. These were later considered too close to workflow diagrams and an additional actor-transaction diagram has been added.

3. Shall the Content Creator Actor be a Document Source Actor instead? In this profile there is no responsibility for the Content Creator to be a repository; in other words it does not need to support an unsolicited request for a document. It is not clear to me if the Content Creator is also responsible for supporting unsolicited requests for a document.

Response to Issue 3: The Content Creator is not required to support unsolicited requests for the content it created. F2F 4/27/2015.

4. Is the CommunicatePDCData SOAP action (defined by PDC) used in any IHE profiles?

Response to Issue 4: It appears to be used only by PCHA.

1. How should we partition this profile? At present, it is one profile containing content from PCC and PCD. Should it be restructured as was done for Radiology Clinical Decision Support/PCC Guideline Appropriate Ordering? Is this a PCC or PCD profile in the end?
2. Related to #1: Should Communicate PCHA Data be a PCD or PCC transaction?
3. How shall the different Communicate PCHA Data-* transactions be described in Vol 2. The issue is that the IEEE-based transactions are identical except for transport and for all IEEE capable transports are referenced in the same documents.

Response to Issues 1, 2, and 5: PCC to own pointing to Continua Guidelines. Continua to maintain.

General Introduction

Appendix A – Actor Summary Definitions

Actor	Definition
Sensor Data Source	This actor is the Personal Healthcare Devices (PHD) generating sensor data
Sensor Data Consumer	This actor receives sensor data from Personal Healthcare Devices (PHDs)

Appendix B – Transaction Summary Definitions

Communicate PCHA Data [PCC-15] – These transactions contain the discrete data from the remote Personal Health Device, such as device identification data, data related to the settings and calibration of the device, and the sensor data itself over at least one of several transport options. The transaction supports five transport options. To qualify as PCHA data certain time stamping requirements must be met; e.g., all stored data must be time stamped and any device containing timestamps in the measurements must expose its sense of current time and its time synchronization (if any).

Communicate PCD Data-hData [PCC-21] – This transaction contains the PCD-01 message generated from sensor data using RESTful POST transports. The uploading side of the transaction cannot assume that the consumer persists data.

Communicate PCD Data-SOAP [PCC-22] – This transaction contains the PCD-01 message generated from sensor data using Web Services. The uploading side of the transaction cannot assume that the consumer persists data.

Communicate FHIR Data-hData [PCC-42] – This transaction contains a complete FHIR bundle generated from sensor data using RESTful POST transports. By 'complete' is meant that is has all the information content that would have been present in the PCC-21 transaction PCD-01 message. The uploading side of the transaction cannot assume that the consumer persists data.

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

Glossary Term	Definition
AHD	Application Hosting Device. Old name for a PCHA PHG.
BT	Classic Bluetooth (versus BTLE)
BTLE	Bluetooth Low Energy (also called Bluetooth Smart and denoted BLE)
HDP	Health Device Profile. A transport profile defined for classic Bluetooth (BT)
IEEE-11073-20601	Optimized Exchange Protocol. A transport-agnostic packet-based protocol for exchanging health data. Currently used only over local transports (PHCD USB, ZigBee, HDP Bluetooth, NFC)
IHE PCD Data	PCHA sensor data expressed in the form of a PCHA-compliant IHE PCD-01

Glossary Term	Definition
	message.
NFC	Near Field Communication wireless protocol (peer endpoints must almost 'touch' to communicate)
PCHA	Personal Connected Health Alliance (Formally Continua)
PCHA Data	Data arriving over the Continua-specified PCHA Transaction from PHD devices. This data is typically provided by sensors and contains sufficient information to generate the non-demographic components of and enterprise time requirements for the IHE PCD-01 or PHMR modules.
PHDC	Personal Health Device Class. A transport profile defined for USB.
PHMR	Personal Healthcare Monitoring Report. A C-CDA document designed primarily to record medical measurements taken on a patient by a sensor device.
PHD	Personal Health Device such as a pedometer, glucometer, blood pressure cuff, thermometer, etc.
PHG	Personal Health Gateway such that collects PHD data and delivers it to, often remotely located, destinations. Formerly known as an AHD.
PM Store	Persistent Metric (PM) data Storage. An IEEE 11073 20601 means of persistently storing measurement data and exposing it to a peer.
RESTful POST	Terminology used by the RPM Profile to indicate the use of only the RESTful create (HTTP POST) operation of the data to a server. It is not fully 'RESTful' in the sense that no further RESTful transactions or RESTful hierarchies are supported. An important aspect of the use of this term in the RPM Profile is that there is no assumed persistence of the uploaded data.
RESTful FHIR	Terminology used by the FHIR standard to indicate compliance to the FHIR RESTful API and FHIR resource model. An additional important aspect of the use of this term in the RPM Profile is that the FHIR server persists uploaded resources.
RPM	Remote Patient Monitoring
USB	Universal Serial Bus
ZB	ZigBee wireless protocol

Volume 1 – Profiles

Copyright Licenses

Add the following to the IHE Technical Frameworks General Introduction Copyright section:

NA

Domain-specific additions

NA

Add Section X

X Remote Patient Monitoring (RPM) Profile

The Remote Patient Monitoring Profile describes a standardized means to transmit measurements taken by personal healthcare devices in a remote setting to a health care provider, including remote home monitoring, sub-acute therapy devices and wearable technologies. Remote in this case means outside of a care provider facility and is typically in the patient's home. In this manner, a patient's status can be monitored without repetitively travelling to a provider facility until deemed necessary, reducing interference in their day to day lives. In addition patients can be in an environment that they are more familiar and comfortable with. The reduction of personal stress and overall expense is especially beneficial in the case of independent living support, chronic disease management and post-operative recovery.

This profile is, for all practical purposes, an expression of the already existing set of standards and interfaces defined by PCHA for the delivery of remote patient data taken by Personal Healthcare Devices to the care provider in terms of IHE actors and transactions. No new standards or transactions are proposed.

The typical technology used to support remote monitoring includes:

- A Personal Health Device (PHD) which produces various health-related measurements through different kinds of sensors, and
- A collector that gathers data from one or more PHDs and forwards the information to a health information exchange or directly to the health care provider's electronic health record or care management system, and/or
- The health information exchange that makes the data accessible to healthcare providers such as the physician or care coordinator, and
- An electronic health record or care management system that provides healthcare providers or coordinators with access to the patient's health record and monitoring data.

Personal health devices include sensors such as a weight scale, SpO_2 sensors, blood pressure cuffs, and medication dispensers. These devices connect to a data collector using a variety of personal networking protocols, such as Bluetooth®, ZigBee®, and USB connections. Personal health devices tend to use embedded systems to handle data communication, and have limited capabilities. They may not even have a clock to keep track of the date and time a measurement is taken.

Collectors are typically applications built into devices such as a set-top box attached to a cable or local area network, a personal computer, or a mobile device such as a cellular phone or tablet. These applications collect data from one or more PHDs and send them on to the healthcare provider either directly or via a health information exchange.

Health information exchanges in the RPM Profile are typically servers used to coordinate and manage large numbers of remotely located collectors and transform and transmit the collected data into the desired content for the consumer. Since the health information exchange is not required to persist data in the management and translation process it reduces the chance of exposing personal health information.

The Remote Patient Monitoring Profile uses transactions that include the transport of data content based on IEEE 11073 terminologies for remote patient monitoring devices. Please see the list of terminologies in Appendix A.

X.1 RPM Actors, Transactions, and Content Modules

This section defines the actors, transactions, and/or content modules in this profile. General definitions of actors are given in the Technical Frameworks General Introduction Appendix A at http://ihe.net/Technical_Frameworks.

The intent of the RPM Profile is to standardize the representation of device observations and the transactions necessary to get the device observations to the health care provider. This standardization ensures plug and play operation for each component participating in the RPM Profile from the sensor device (Sensor Data Source) used by the remotely located patient to the EHR document reader used by the health care provider.

The profile consists of the following actors:

1. Sensor Data Source which is typically the Personal Health Device (PHD) sensor
2. Sensor Data Consumer that receives the data from the sensor device. In this profile, the Sensor Data Consumer must be grouped with either a Device Observation Reporter or Content Creator.
3. Device Observation Reporter that generates a PCD-01 message and/or complete FHIR Bundle from the PCHA data.
4. Device Observation Consumer that receives the PCD-01 message and or complete FHIR Bundle from the Device Observation Reporter. In the RPM Profile, the Device Observation Consumer must be grouped with a Content Creator that creates PHMR content and/or FHIR resource content from IHE PCD-01 or complete FHIR Bundle data. In some use cases the delivery of the data as a PCD-01 message or complete FHIR Bundle may suffice, however to participate in this profile such a module must also expose a repository that can be used by other IHE profiles.
5. Content Creator that generates a PHMR content module or FHIR resources and makes that Content available to a Content Consumer. A Content Consumer that delivers the PCD-01 message as content is also being considered.
6. Content Consumer that receives a PHMR content module or FHIR resources. A module consisting of a Content Consumer and Device Observation Reporter that does not expose its content to other IHE profiles is currently out of scope of the RPM.

The profile also consists of the following transactions where the '*' in the name indicates one of several possible transports:

1. Communicate PCHA Data transaction communicates sensor data to the appropriate consumer over five possible transports
2. PCD-01 Communicate PCD Data-* transaction communicates a PCD-01 message to the appropriate consumer over two possible transports

3. Communicate FHIR Data transaction communicates a complete FHIR Bundle to the appropriate consumer over RESTful POST transports
4. PCC Document Sharing transaction distributes the PHMR content module by an agreed upon technique (such as XDS.b or XDM) to an appropriate consumer
5. PCC FHIR Resource Sharing transaction delivers FHIR resources to a FHIR server using the RESTful FHIR API.

The profile also consists of the following Content Modules:

1. Personal Healthcare Monitoring Report (PHMR).
2. PCHA FHIR resources

Figure X.1-1 shows the actors and actor groupings directly involved in the RPM Profile and the relevant transactions between them. The dotted boxes indicate actors that are required to be grouped with the actor in the solid box.

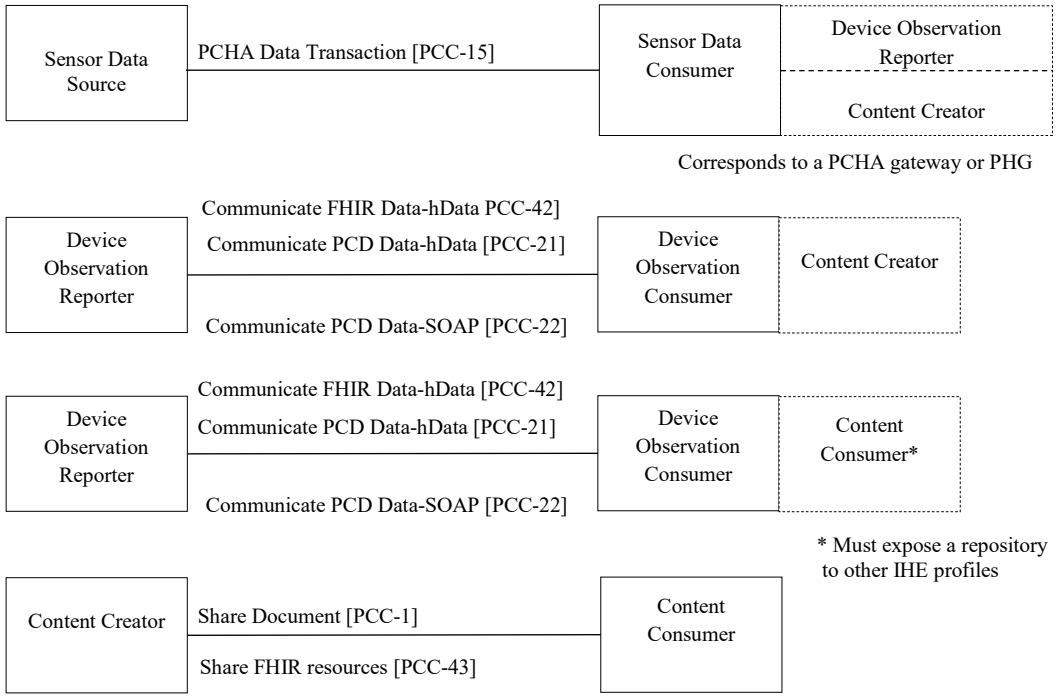


Figure X.1-1: RPM Actor Diagram

Figure X.1-2 shows the end to end implementation options of this profile. In some sense the figure indicates a 'workflow' though all the stages (once initiated) are automated. It is envisioned

that the two primary end to end implementations consist of (1) the four-module version where the Sensor Data Source Actor is one component, the Sensor Data Consumer and Device Observation Reporter Actor group is a second component, the Device Observation Consumer and Content Creator Actor group is a third component and the Content Consumer is the fourth component and (2) the three-module version where the Sensor Data Source Actor is one component, the Sensor Data Consumer and Content Creator is a second group, and the Content Consumer is the third group. The first case is expected when the content to be generated is a PHMR, and the second is anticipated when the content generated is FHIR resources. The separate 'sensor' box in the figure indicates the presence of some hardware that is capable of taking medical measurements. Alternative deployments of this profile that combine the above components such that the total number of transactions is reduced are also shown using boxes with thinner lines. For the most part, costs and maintenance issues make the alternative deployments less attractive. However, with the increased ubiquity of mobile devices and the introduction of FHIR, combining the sensors with Device Observation Reporter Actors or combining the Content Module with the Device Observation Consumer onto these mobile platforms is a likely development.

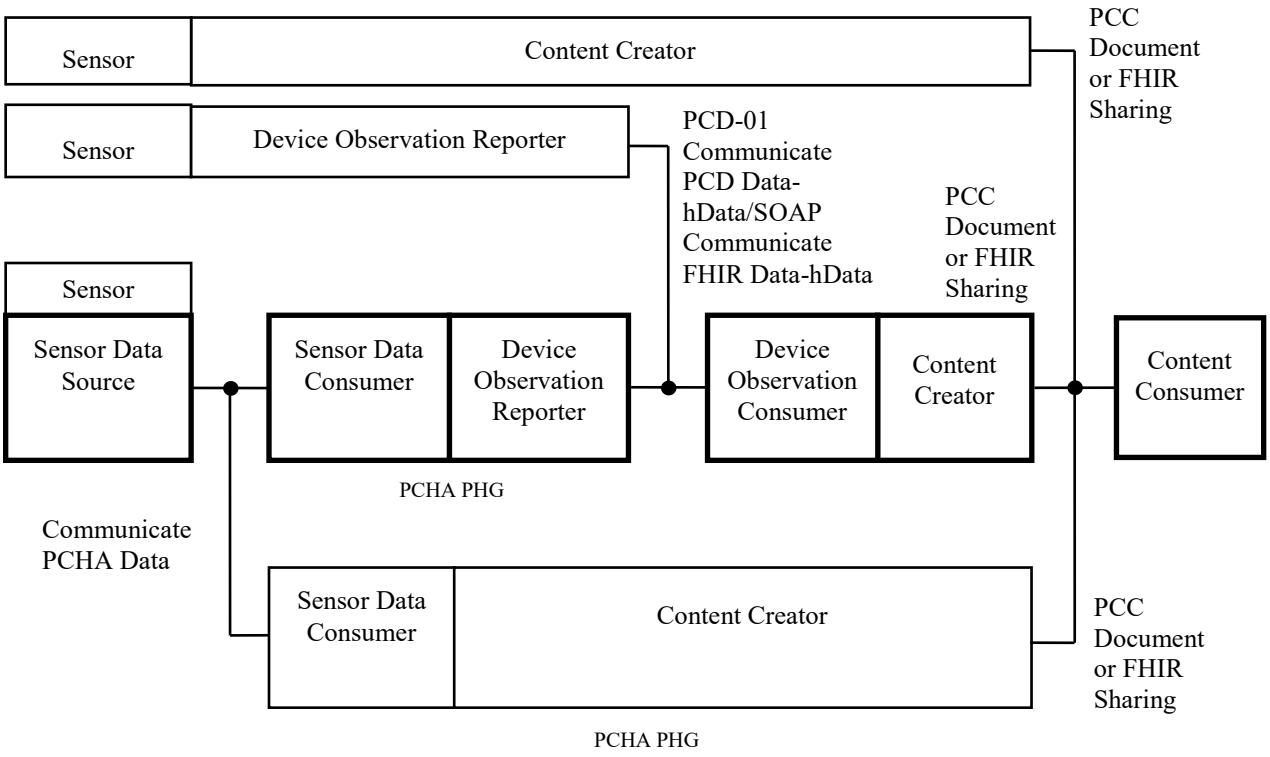


Figure X.1-2: RPM End-to-End 'Flow' Diagram

The equivalent PCHA end-to-end data flow that is analogous to the four component deployment in Figure X.1-2 is shown in the Figure X.1-3. It should be noted that PCHA also defines the same alternative deployments as shown in Figure X.1-2 except for a sensor device acting as a Content Creator.

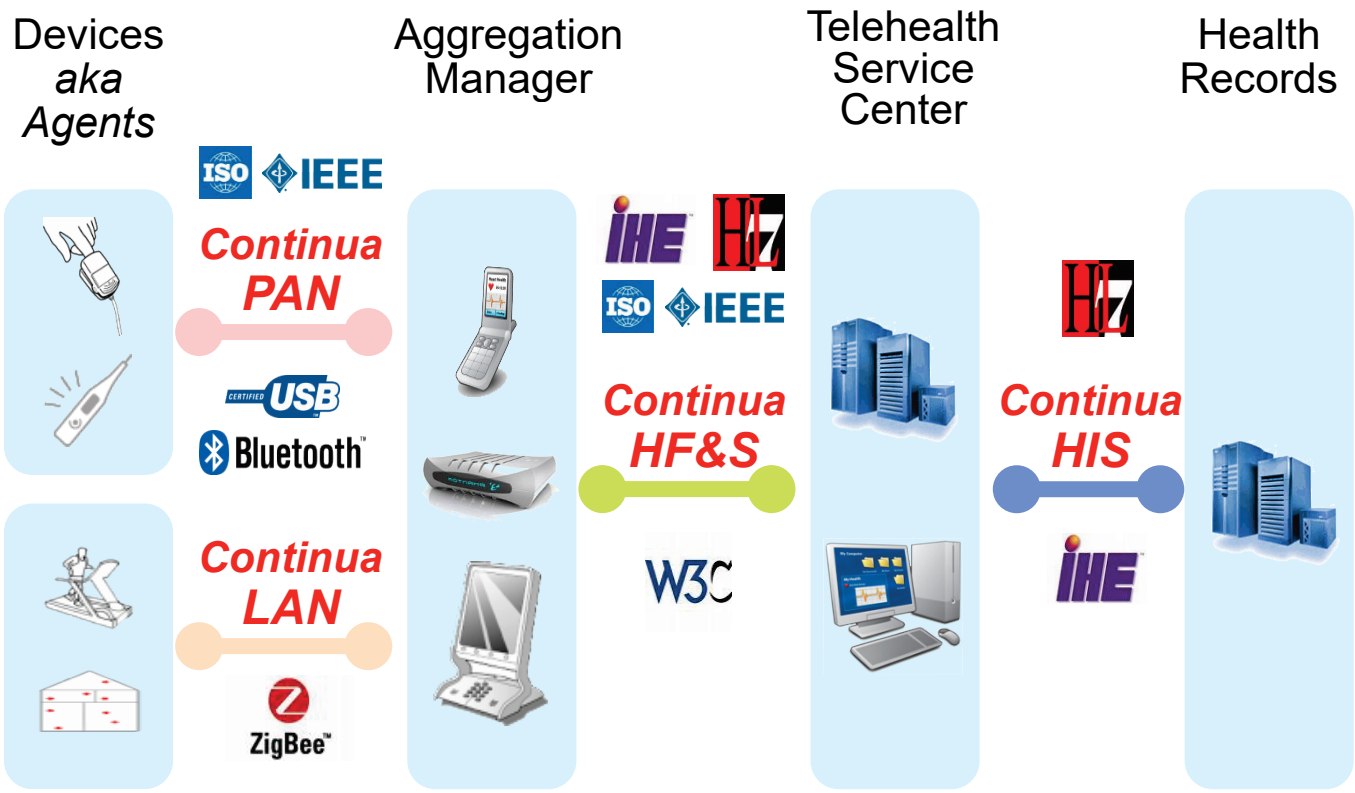


Figure X.1-3: PCHA End-to-end Flow Diagram

Table X.1-1 lists the transactions for each actor directly involved in the RPM Profile. To claim compliance with this profile, an actor shall support all required transactions (labeled "R") and may support the optional transactions (labeled "O").

Table X.1-1: RPM Profile - Actors and Transactions

Actors	Transactions	Optionality	Reference
Sensor Data Source	Communicate PCHA Data BT (HDP Bluetooth)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data USB (PHDC USB)	O[1]	PCC TF-2: 3.15

Actors	Transactions	Optionality	Reference
	Communicate PCHA Data ZB (ZigBee)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data NFC (Near Field Communication)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data BTLE (Bluetooth Low Energy)	O[1]	PCC TF-2: 3.15
Sensor Data Consumer	Communicate PCHA Data BT (HDP Bluetooth)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data USB (PHDC USB)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data ZB (ZigBee)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data NFC (Near Field Communication)	O[1]	PCC TF-2: 3.15
	Communicate PCHA Data BTLE (Bluetooth Low Energy)	O[1]	PCC TF-2: 3.15
Device Observation Reporter	Communicate PCD Data-SOAP (Web services) [PCD-01]	O[1]	PCD TF-2: 3.22
	Communicate PCD Data-hData (RESTful transport) [PCD-01]	O[1]	PCD TF-2: 3.21
	Communicate FHIR Data-hData (RESTful transport)		PCD TF-2: 3.42
Device Observation Consumer	Communicate PCD Data-SOAP (Web services) [PCD-01]	O[1]	PCD TF-2: 3.22
	Communicate PCD Data-hData (RESTful transport) [PCD-01]	O[1]	PCD TF-2: 3.21
	Communicate FHIR Data-hData (RESTful transport)	O[1]	PCD TF-2: 3.42
Content Creator	Document Sharing [PCC-1]	O[2]	PCC TF-3: 6.3.1
Content Creator	FHIR resource Sharing [PCC-43]	O[2]	PCC TF-3: 6.6.6- PCC TF-3: 6.6.18, PCC TF-3: 6.7.1, PCC TF-3: 6.7.2 PCC TF-3: 6.8.1- PCC TF-3: 6.8.2
Content Consumer	Document Sharing PHMR [PCC-1]	O[2]	PCC TF-3: 6.3.1

Actors	Transactions	Optionality	Reference
Content Consumer	FHIR resource Sharing [PCC-43]	O[2]	PCC TF-3: 6.6.6- PCC TF-3: 6.6.18, PCC TF-3: 6.7.1, PCC TF-3: 6.7.2 PCC TF-3: 6.8.1- PCC TF-3: 6.8.2

[1] At least one transport must be supported.

[2] At least one content type must be supported.

Table X.1-2: RPM Profile - Actors and Content Modules

Actors	Content Modules	Optionality	Reference
Content Creator	PHMR	O[1]	PCC TF-3: 6.3.1.D
Content Creator	FHIR resources	O[1]	PCC TF-3: 6.6
Content Consumer	PHMR	O[1]	PCC TF-3: 6.3.1.D
Content Consumer	FHIR resources	O[1]	PCC TF-3: 6.6

[1] At least one of the content types must be supported.

X.1.1 Actor Descriptions and Actor Profile Requirements

The RPM Profile consists of the following actors:

1. Sensor Data Source Actor which is typically the Personal Health Device (PHD) sensor
2. Sensor Data Consumer Actor that receives the data from the sensor device. In this profile, the Sensor Data Consumer must be grouped with either a Device Observation Reporter or Content Creator Actor.
3. Device Observation Reporter Actor that generates a PCD-01 message or complete FHIR Bundle from the PCHA data
4. Device Observation Consumer Actor that receives PCD-01 messages or complete FHIR Bundles from the Device Observation Reporter Actor. In this profile, the Device Observation Consumer Actor is grouped with a Content Creator Actor that creates PHMR content and/or FHIR resource modules from IHE PCD-01 data or complete FHIR bundles.
5. Content Creator Actor that generates a PHMR content and/or FHIR resource modules and makes that Content available to a Content Consumer.

6. Content Consumer Actor that can utilize a PHMR content module or FHIR resource modules.

A product that claims conformance to this profile could implement one of the following actors or actor groups:

1. A sensor device acting as a Sensor Data Source supporting one or more transports
2. A sensor device acting as a Device Observation Reporter supporting one or both transports (hData/SOAP)
3. A sensor device acting as a Content Creator
4. A Sensor Data Consumer supporting one or more transports grouped with a Device Observation Reporter supporting one or both transports (a PCHA PHG)
5. A Sensor Data Consumer grouped with a Content Creator (a PCHA PHG)
6. A Device Observation Consumer supporting one or both transports grouped with a Content Creator
7. A Device Observation Consumer supporting Content Consumer that exposes content to other IHE profiles.
8. A Content Consumer capable of reading a PHMR and/or FHIR resources

These components do not rule out an implementation where a manufacturer implements, for example, a Sensor Data Consumer grouped with both a Device Observation Reporter and Content Creator. Such a component could provide both a PCD-01 message and/or PHMR and/or FHIR resource content modules.

Clearly for interoperability, peer implementations must support the same transports.

Due to resource requirements, costs, and maintenance efforts, it is envisioned that the most common set of components satisfying the end-to-end nature of this profile when the end content generated is a PHMR will consist of one or more Sensor Data Source components and a Sensor Data Consumer grouped with a Device Observation Reporter component for each patient, and a Device Observation Consumer grouped with a Content Creator component serving several patients sharing PHMR content modules with several Content Consumers. When the end content is FHIR resources, the set of components satisfying the end-to-end nature of this profile may skip the Device Observation Reporter and Device Observation Consumer interface, but for management purposes and the protection of Personal Health Information, the former approach may still be more appropriate.

The transactions involved in this profile utilize multiple transports.

The Communicate PCHA Data transaction specified by the PCHA H.811-TAN-PAN-LAN Interface guidelines currently supports the following transports and protocols

- IEEE 11073-20601 packets over
  - HDP Bluetooth

- PHDC USB
- ZigBee
- NFC

- Assorted Health device profiles overs Bluetooth Low Energy Generic Attribute (GATT) protocol

The PCHA guidelines place further requirements upon these protocols and transports than defined in the respective IEEE 11073 20601 and corresponding specialization specifications and the Bluetooth Low Energy health device profiles and services. The Sensor Data Source Actor implementing these transactions must provide what is referred to as PCHA data in this specification. The PCHA data is required to have certain device information and (conditionally) timing information to allow generation of observation data that can be coordinated and corrected to a UTC synchronized time source by the Sensor Data Consumer / Device Observation Reporter Actor group if the Sensor Data Source has not already done so. In particular, any stored measurements MUST provide a time stamp, and any Sensor Data Source Actor providing a timestamp in any measurement (stored or live) MUST provide its sense of current time. PCHA has certification requirements on a per-transport basis for this transaction for both the Sensor Data Source and Sensor Data Consumer.

The PCD-01 Communicate PCD Data-hData and PCD-01 Communicate PCD Data-SOAP transactions communicate observation data in the form of a PCD-01 message to an appropriate consumer. The transaction uses one of the following transport methods:

- Continua PCHA hData Observation-Upload
- Continua PCHA SOAP Observation-Upload

as specified in the PCHA H.812.1 - Observation Upload and PCHA H.812-WAN Interface guidelines. The SOAP Observation-Upload uses the web services based IHE CommunicatePCDData SOAP action over TLS authenticated with SAML. The hData Observation-Upload uses RESTful POST transports over TLS authenticated by oAuth. How the SAML or oAuth tokens are obtained is not specified by this profile but is a business decision made by the communicating partners.

The Communicate FHIR Data-hData transaction communicates observation data in the form of a complete FHIR Bundle to a Device Observation Consumer. The transaction is identical to the Communicate PCD Data-hData transaction where a complete FHIR Bundle replaces the PCD-01 V2 message. The FHIR Bundle has the same semantic content as the PCD-01 message but uses the FHIR data model and syntax.

The PCC Document Sharing transaction uses any IHE specified transport method that is capable of sharing a PHMR document. The PCHA H.813 - HIS Interface guidelines restricts the transaction to IHE XDR, XDS (XDS.b Provide and Register Document Set) or IHE XDM. It is expected to soon include DIRECT as well. These transports communicate the PHMR C-CDA content module to the consumer.

The PCC FHIR Resource Sharing transaction shares FHIR resources in lieu of a PHMR document. The sharing transaction uses RESTful FHIR in the context of TLS oAuth security. Additional constraints are placed upon the transaction by PCHA H.812-5, the majority of which are to prevent resource duplication, personal health information protection, security, and reduction of bandwidth.

Details of these requirements are documented in Transactions (Volume 2) and Content Modules (Volume 3). This section documents any additional requirements on the RPM Profile's actors.

X.1.1.1 Sensor Data Source

Typically, the Sensor Data Source Actor is a Personal Health Device (sensor) which captures measurements about a patient. These measurements are communicated to the Sensor Data Consumer using one or more of the protocols and transports specified in the Communicate PCHA Data transaction as described below.

X.1.1.2 Sensor Data Consumer

The Sensor Data Consumer Actor receives data from the sensor. The data is augmented with personal information and any timing issues are corrected and coordinated. The data is subsequently forwarded to the healthcare provider. In this profile, the Sensor Data Consumer must be grouped with either a Device Observation Reporter or Content Creator Actor to handle the forwarding of the information.

The Device Observation Reporter associates the sensor data with a time stamp, and the patient identity. PHD sensors typically can be used by multiple patients (e.g., a weight scale), and so the Sensor Data Consumer may need to distinguish which patient the device is currently measuring. Sensors may not keep track of time and date when sending data in real time, so the Sensor Data Consumer must time stamp the measurements. The Device Observation Reporter should, but is not required to support the IHE Time Client Actor of the Consistent Time protocol. These devices may be wirelessly connected devices which get their time from the cellular network, rather than from an NTP or SNTP server.

X.1.1.3 Device Observation Reporter

The Device Observation Reporter Actor is responsible for transmitting augmented sensor observations one step closer to the healthcare provider.

X.1.1.4 Device Observation Consumer

The Device Observation Consumer accepts augmented device observations. It must be grouped with a Content Creator Actor or a Content Consumer Actor that exposed content to other IHE profiles. The Content Creator forwards the augmented device observations to the healthcare provider.

X.1.1.5 Content Creator

The Content Creator formats sensor data in the Personal Health Monitoring Report (PHMR) format specified in *HL7® [2]CDA R2 Implementation Guide: Personal Healthcare Monitoring Reports, Release 1*, a form suitable for consumption by EHR, HIE and other Health IT systems, and which is also human readable. Alternatively, or additionally, the augmented device observations may be formatted as FHIR resources and transmitted to a FHIR server as specified by Continua Design Guideline H.812.5.

X.1.1.6 Content Consumer

The Content Consumer Actor is used by the healthcare provider to access stored sensor data associated with a patient in the Personal Health Monitoring Report (PHMR) format or as FHIR resources.

X.2 RPM Actor Options

Options that may be selected for each actor in this profile, if any, are listed in the Table X.2-1. Dependencies between options when applicable are specified in notes.

Table X.2-1: PRM - Actors and Options

Actor	Option Name	Reference
Sensor Data Source	Communicate PCHA Data BT	PCC TF-2: 3.15
	Communicate PCHA Data USB	PCC TF-2: 3.15
	Communicate PCHA Data ZB	PCC TF-2: 3.15
	Communicate PCHA Data NFC	PCC TF-2: 3.15
	Communicate PCHA Data BTLE	PCC TF-2: 3.15
Sensor Data Consumer	Communicate PCHA Data BT	PCC TF-2: 3.15
	Communicate PCHA Data USB	PCC TF-2: 3.15
	Communicate PCHA Data ZB	PCC TF-2: 3.15
	Communicate PCHA Data NFC	PCC TF-2: 3.15
	Communicate PCHA Data BTLE	PCC TF-2: 3.15
Device Observation Reporter	PCD-01 Communicate PCD Data-SOAP	PCC TF-2: 3.22
	PCD-01 Communicate PCD Data-hData	PCC TF-2: 3.21
	Communicate FHIR Data-hData	PCC TF-2: 3.42
Device Observation Consumer	PCD-01 Communicate PCD Data-SOAP	PCC TF-2: 3.22

[2] HL7 is the registered trademark of Health Level Seven International.

Actor	Option Name	Reference
	PCD-01 Communicate PCD Data-hData	PCC TF-2: 3.21
	Communicate FHIR Data-hData	PCC TF-2: 3.42

Note: Each actor must support at least one of the transaction transports.

X.3 RPM Required Actor Groupings

An actor from this profile (Column 1) shall implement all of the required transactions and/or content modules in this profile ***in addition to*** all of the transactions required for the grouped actor (Column 2).

Section X.5 describes some optional groupings that may be of interest for security.

Table X.3-1: RPM - Required Actor Groupings

RPM Actor	Actor to be grouped with	Reference	Content Bindings Reference
Sensor Data Consumer[1]	Device Observation Reporter	PCC TF-1: X.3.2	<Reference to CM bindings section e.g., <Domain Acronym TF-3:Z.xxx > (e.g., PCC TF-2 :4.1)
Sensor Data Consumer[1]	Content Creator	PCC TF-1: X.3.2	
Device Observation Consumer	Content Creator	PCC TF-1: X.3.3	
Device Observation Consumer	Content Consumer* *Must expose content to other IHE profiles	PCC TF-1: X.3.3	
Sensor Data Source	None	PCC TF-1: X.3.1	
Device Observation Reporter	None	PCC TF-1: X.3.4	
Content Creator	Consistent Time	PCC TF-1: X.3.5	
Content Consumer	None	PCC TF-1: X.3.6	

Note 1: The Sensor Data Consumer is required to be grouped with *either* the Device Observation Reporter or Content Creator. It *may* be grouped with both.

The Content Creator in this profile depends upon the Consistent Time Profile. Table X.3-2 defines the dependency:

X.3.1 Sensor Data Source

This actor has no required grouping.

X.3.2 Sensor Data Consumer

The RPM Profile as defined in this document is the first stage in providing a standardized means

Table X.3-2: Content Module Dependencies

Integration Profile	Depends on	Dependency Type	Purpose
Remote Patient Monitoring Profile (RPM)	Consistent Time	The Content Creator implementing this profile must implement the Consistent Time Profile.	Required for consistent time-stamping of the PHMR content module and the FHIR Observation resources.

X.4 RPM Overview

The RPM Profile describes a set of standardized means to deliver patient health measurements and monitoring data in a remote setting to a health care provider. The delivery route can take one of several paths. The delivery path as illustrated in Figure X.4-1 shows the path where a backend is used to coordinate data from multiple remote collectors and dispatch the data in the desired form to the EHR.

In this case there are several monitored patients, each with their own set of sensor devices and a local collector of those sensor observations. Each collector then sends its clinical data to a single back end server that generates the content appropriate for one of several consumers.

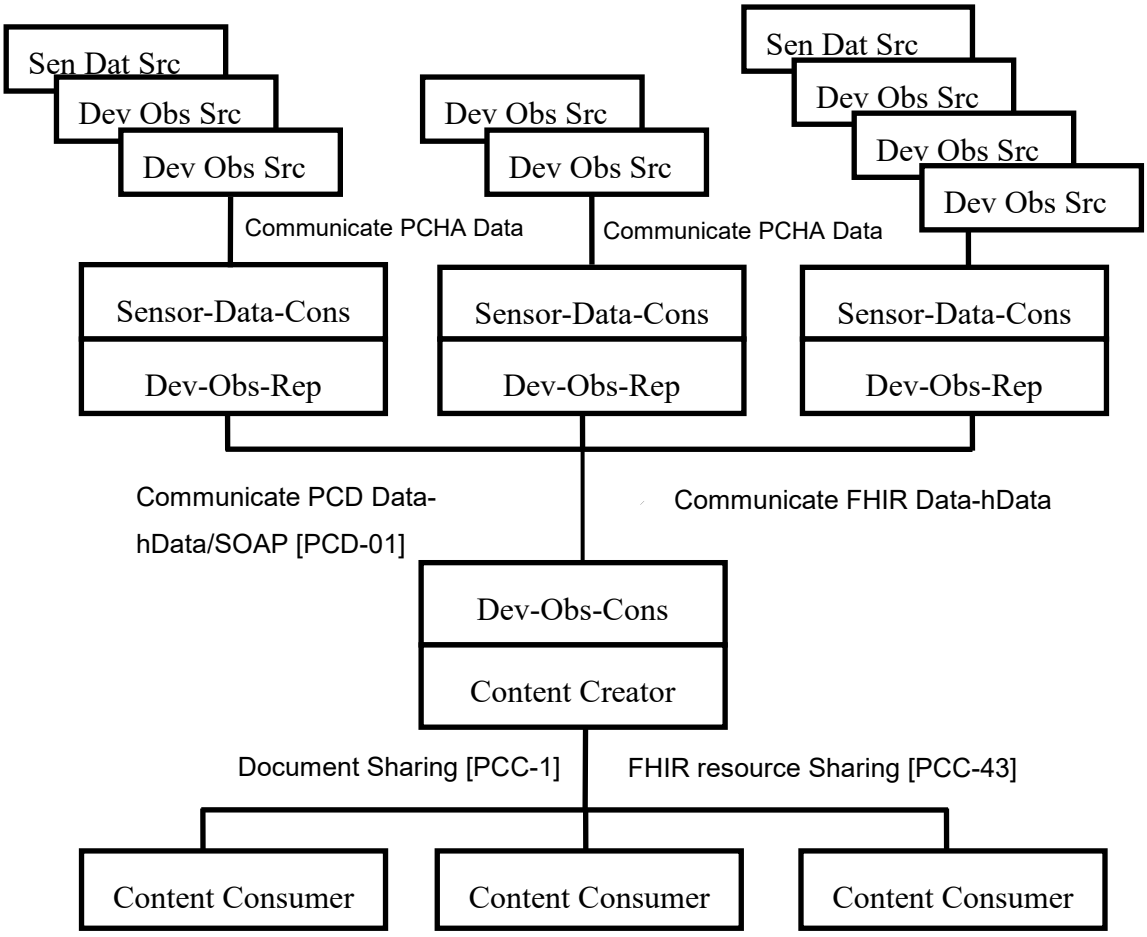


Figure X.4-1: RPM Operational Diagram

There are a couple of reasons that a business use case may implement the RPM Profile as indicated in Figure X.4-1. First, the collector of sensor observations is typically done on low-footprint hardware, such as a mobile phone, tablet, or set-top box. Supporting the PHMR and even FHIR resource Content Creator is resource and power demanding making such collectors more expensive. Second, in the case of the PHMR, the amount of supplementary information needed to support the headers of the PHMR content module is quite large compared to the amount of supplementary information needed to support the data coming from the sensor. The task of maintaining and configuring this information then needs to be done for each patient on more expensive hardware if implemented on the local collector. Having a single high end back-end server handling multiple patients and the Content Creator is likely less expensive and easier to maintain. It also allows for a single access point to filter the data that is reported in the Content Module. The filtering can be configured for all patients using the backend instead of each individual collector. In addition, any changes that might be needed (such as in the filtering) are

easier to manage on one backend rather than numerous remotely located collectors. It should be noted that any filtering is an application option established through business needs and is outside the scope of the RPM Profile. Of course, any filtering must still result in a compliant Content Module.

In the case where the Content Module is generating FHIR resources, the amount of additional data needed to supplement the sensor data is no more than that needed in the PCD-01 message. This fact, along with the greater simplicity of acceptable FHIR formats opens up its use on platforms with fewer resources such as a PCHA PHG.

Home sensor devices also need to be low footprint, where the bulk of their expense is the sensor itself. The hardware necessary to support transaction protocols and external configuration is minimized. Since many of the sensor devices may be borne on the patient, making the sensor as small and as unobtrusive as possible also limits hardware resources and power demands. These demands make the Communicate PCHA data transaction the most likely solution for these devices.

In addition, personal health device data is time stamped with a consistent enterprise time. For most sensor applications providing a consistent enterprise time is too costly and too power demanding. Consequently, this time stamping is typically done by the Device Observation Reporter obtaining the PCHA data from Sensor Data Consumer.

X.4.1 Concepts

The RPM Profile as defined in this document is the first stage in providing a standardized means of monitoring patients outside the care provider facilities. This profile currently specifies the transfer of monitoring data from the remote site to the health care facility. PCHA is currently implementing standards for two-way monitoring in the form of consent, questionnaires, IEEE 11073 20601 command and control, and automated persistent sessions. It is anticipated that these standards will either provide enhancements to the RPM Profile or be the basis for additional IHE profiles related to the remote monitoring of patients.

X.4.2 Use Cases

The generic use case for the RPM Profile is any situation in which the health care provider judges that the patient will benefit from being able to be medically and environmentally monitored outside of the health care facility (typically the home). Quality of life and reduction in costs are also important factors in the judgment. Financial stress is a realistic concern for many patients.

X.4.2.1 Use Case #1: Chronic Disease Management

Chronic Disease Management allows compromised individuals managing disorders such as diabetes, hypertension, heart disease, sleep apnea, etc. to go through their daily lives with as minimal intrusion as possible. The RPM Profile allows a greater number of such people to live as normal a life as possible.

X.4.2.1.1 Chronic Disease Management Use Case Description

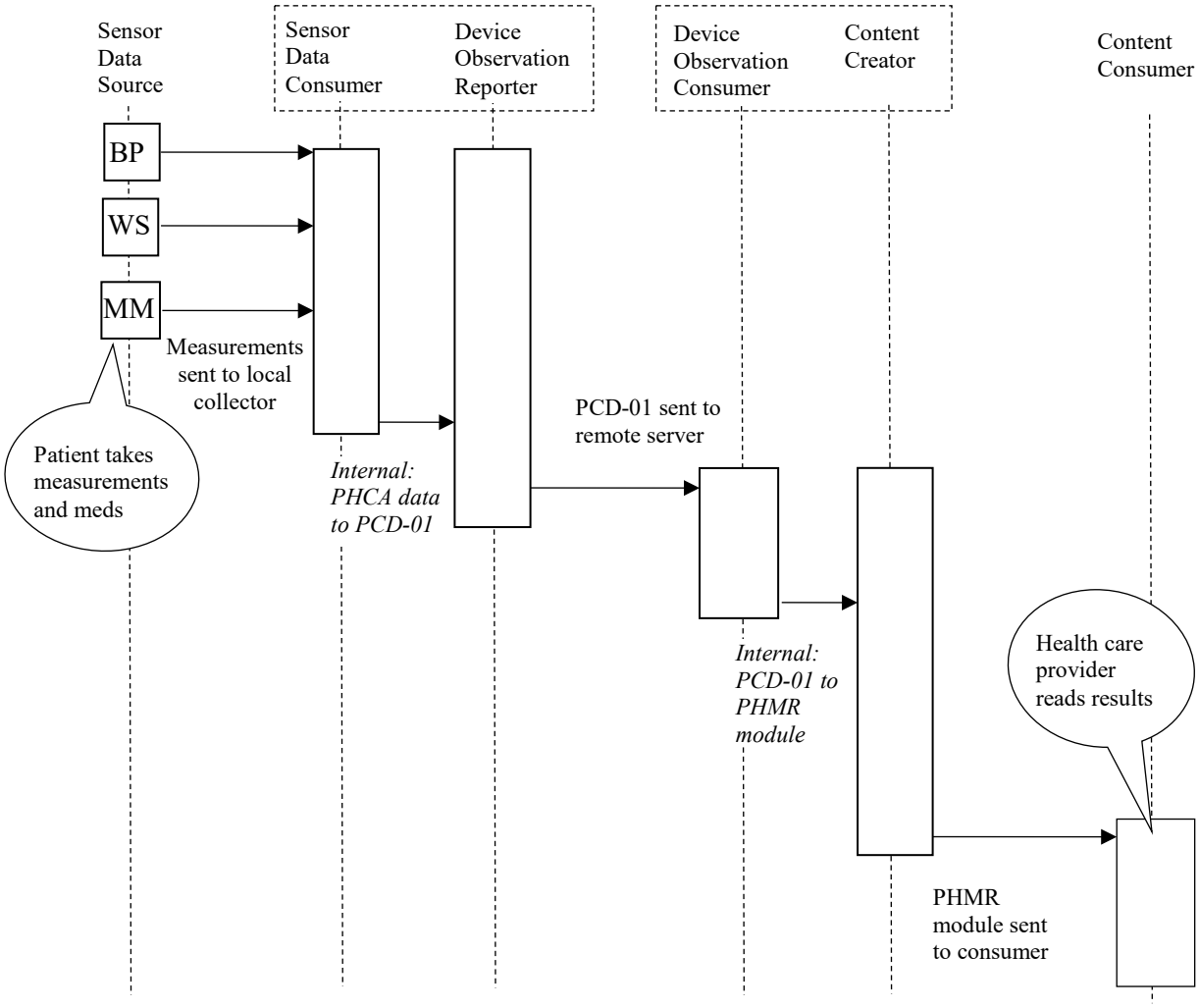
People can become physically and medically compromised for several reasons. However, in many cases these people would be able to live a fairly normal and functional life with minimal intrusion if as much of the continuous monitoring could be done on the person without visits to a professional facility. The patient can transfer monitoring measurements to the health care provider at a pre-determined frequency using the RPM. The health care provider can then decide whether additional monitoring and thus a visit to the provider are warranted.

X.4.2.1.2 Chronic Disease Management Process Flow

A patient suffers from hypertension and is at high risk for stroke. The patient needs to take certain medications each day and ideally needs to lose some weight. The health care professional's institution already has the infrastructure to create, read, and distribute IHE compatible Electronic Heath Records (EHRs) as C-CDAs. The health care professional provides the patient with a blood pressure cuff from BP Manufactures, Inc., a weight scale from WS Solutions, and a medication monitor from AMM GBH containing next month's daily medication doses. All the devices are PCHA compliant. The patient also receives a PCHA compliant set top box from PHG Magic, Inc. The patient was given the choice to use either a set top box or a mobile tablet, the latter of which would display the patient's measurements as received. The patient chose the set top box because the patient is technology challenged and did not want to turn on the device and/or activate the application to see the measurements as they were uploaded from the devices. The chosen set top box is pre-configured to communicate with a PCHA compliant server application developed by Medical Application Services. This application has been installed on a system at the health care provider's facility. The server application has a web interface that allows the health care provider to generate an account for a given patient. The account will contain information about the given patient that the health care facility requires for its record keeping. A user name and password is required to access this account and that information has been configured into the patient's set top box. When the server application receives data from this patient it then knows to generate a PHMR that is delivered to an XDS.b repository the health care provider can access.

The patient has been instructed on how to use the devices and to plug in the set top box in the area where the devices are to be used. Each morning the patient is to take a blood pressure reading, a weight measurement, and the daily medications. When the patient performs these tasks, a PCHA compliant message is sent to the set top box which gives a beep of approval and converted to an IHE PCD-01 message. The first time this is done, the set top box requests the back end server application for a SAML token using the user name and password configured by the health care provider's facility. If correct, the set top box receives the token from the server application and sends the PCD-01 message in a TLS-secured IHE CommunicatePCDData SOAP action authenticated with the SAML token. The server application validates the token and if valid, converts the data to a PHMR module which it then sends to the XDS repository, using the IHE XDS.b provide and register document set transaction, where the health care provider can now read it.

715 In this manner the health care provider can monitor the patient and make medical decisions based on it, allowing the patient to go about his/her daily tasks with minimal intrusion. Remote monitoring does not preclude the patient from directly contacting the health care provider.



720

Figure X.4.2.1.2-1: Basic Process Flow in RPM Profile

X.4.2.2 Use Case #2: Post-Operative Recovery

725 Remote Post-Operative recovery allows a patient to recover from the effects of surgery or other traumatic procedures (such as chemotherapy) amongst family and friends in a familiar environment.

X.4.2.2.1 Post-Operative Recovery Use Case Description

A patient that has had surgery, or chemotherapy, or radiation treatment, or has undergone some other medically traumatic event will often need to be monitored for potential complications. In some cases (such as a broken bone) the potential for complications is so low that it is standard procedure that recovery is at home. In many other cases monitoring is needed but it is fairly simple, and any complications that might be detected from the monitoring will not be acute. Nevertheless, the patient is either required to stay at the facility to receive this monitoring or is required to frequently visit the facility to be monitored, both of which are inconvenient and expensive. If the patient can be provided with the monitoring equipment, recovery can take place in the home and visits to the facility take place only when warranted.

X.4.2.2.2 Post-Operative Recovery Process Flow

A patient has just undergone heart surgery. The surgery appears to have gone well and the patient shows no signs of complications. The care giver provides the patient with a PCHA-compliant weight scale from ViktMasters AB, blood pressure cuff from MedMax Gmbh, pulse oximeter from POSpecialists, Inc., and medication monitor from AMM Masters AB, and installs a PCHA complaint application hosting device application from Medical Mjukvaror AB on the patient's mobile phone. The Medical Mjukvaror PHG application is configured to transfer the data to an application obtained from Medical Servers, Inc. running on the facilities back end server. The health care staff has configured an account for the patient on this server. The care giver instructs the patient to take a weight measurement, blood pressure measurement, and pulse oximeter reading twice a day along with medication instructions; once in the morning, and once in the evening. Taking additional weight measurements during other times of the day is encouraged. The patient is instructed to first turn on the mobile device, start the installed Medical Mjukvaror PHG application, and then use the three provided devices to take the measurements. Medications are dispensed from a special pill box. The patient is given a few practice sessions with the devices, the use of the medication dispenser, and mobile phone application. Everything goes smoothly though it takes some extra effort to get used to taking blood pressure measurements. The patient sees the measurements displayed and medications taken on the mobile device and an indication that the data is dispatched to the care provider. The care provider then accesses the data from the examination room terminal and shows the patient the sent measurements.

Once home the patient follows the care giver's instructions; turn on the mobile device, start the PCHA complaint application, and then take the three instructed measurements and the prescribed medications. All devices use the Communicate PCHA Data-BT transaction (Bluetooth) to transfer the measurements and medication indications to the mobile device.

The mobile device then uses the SOAP Observation upload transaction and sends this data as a PCD-01 message to the backend server. The backend server then converts the PCD-01 message to a PHMR module using the supplementary information entered for this patient in the patient's account and uses XDS.b Provide and Register Document Set transaction to send the document to the care provider's repository where it can be examined with the facilities' existing infrastructure.

X.4.2.3 FHIR Usage

In either of the use case scenarios above, uploading FHIR resources to a FHIR server can replace the PHMR and CDA repository and the FHIR data model can be used in place of the PCD-01 V2 message. Neither of these technology changes alter the use case for those involved.

X.5 RPM Security Considerations

Personal Health Devices are typically simple applications embedded with a sensor that communicate to more complex devices through secure wireless personal networking protocols, or connected to devices through a wired USB connection under the control of the user. While they can store data (e.g., a glucose monitor), many rarely store data for other than a short period of time, and only that data that is measured by the sensor. In addition, Personal Health Devices rarely have personally identifiable information as there is currently no standardized means to transmit such information using the Communicate PCHA Data-* transactions. The devices are subject to typical security concerns, such as theft or loss. The main security concern for these devices is their communication channel with other actors. This profile mandates the use of secured network communications when the device is accessed or transmits data through wireless protocols. This mitigates the risk of data interception, interference, or alteration in transit. It is presumed that the device is under user control when it is attached via a wired connection, and so no encryption is required in this case.

Unlike sensors, data collectors may store both sensor data, as well as personally identifiable information, and will communicate it to upstream systems. Like PHDs, these devices are also subject to theft and loss. These devices are required to synchronize time using either native protocols (e.g., through the cellular network that the device is attached), or through use of the IHE Time Client from the Consistent Time Profile. This profile requires the support of encryption of any upstream network transmissions using Transport Layer Security and authentication of the user via SAML when web services are used or oAuth when using RESTful POST as specified in the IHE ITI Technical Framework Supplement: Internet User Authentication (IUA). While audit logging is not required to enable certain kinds of devices the ability to function, they may consider using the Secure Node or Secure Application Actor from the IHE ATNA Profile to ensure that communications are audited, users are authenticated and transmissions are secured between known entities.

Back office, departmental and EHR systems used by the healthcare provider to access the sensor data or translate it to a persistent, human readable format will need to be further secured. See the Security Considerations section for IHE transport protocols used by the Content Creator and Content Consumer Actors (e.g., XDS and XDM) for further details related to those transports. Those transports typically mandate grouping with the Secure Node or Secure Application Actors from ATNA.

RESTful FHIR by itself does not support any security operations, thus in the PCHA guidelines the upload of FHIR resources to a FHIR server supports an oAuth authentication model over TLS. The FHIR server will need to be secured in the same manner as any other EHR system containing personal health data.

X.6 RPM Cross Profile Considerations

NA

Volume 2 – Transactions

3.15 Communicate PCHA Data Transaction [PCC-15]

3.15.1 Scope

This transaction is used to transfer measurement data from Personal Health Device (PHD) Sensor Data Source Actors to an appropriate consumer in a standardized manner. This transaction allows a single Sensor Data Consumer to process data from any compliant sensor device (blood pressure cuffs, glucometers, coagulation meters, sleep apnea breathing therapy equipment, etc.).

This transaction is typically the only point at which a human is involved. Once the measurement data is received by the Sensor Data Consumer, the process of delivering the data to its final destination in its final form at a Content Consumer is automated.

3.15.2 Actor Roles

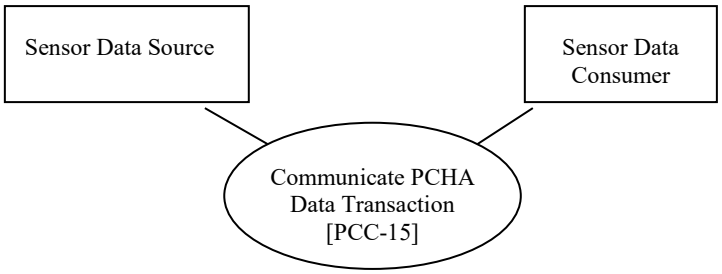


Figure 3.15.2-1: Use Case Diagram

Table 3.15.2-1: Actor Roles

Actor:	Sensor Data Source
Role:	This actor is responsible for taking the measurement on the patient, packaging it into a standardized form and sending it to a consumer in a standardized manner.
Actor:	Sensor Data Consumer
Role:	This actor receives measurement data from one or more Sensor Data Source Actors (sensor devices)

3.15.3 Referenced Standards

The Communicate PCHA data transaction is specified in the following documents:

- *PCHA H.811 - TAN-PAN-LAN Interface*. The PCHA standard relies upon the
  - IEEE 11073 20601 Optimized Exchange Protocol and supporting
    - *IEEE 11073 104xx* device specialization standards
    - Bluetooth transport
      - *Health Device Profile* (Bluetooth SIG) and supporting
      - *Multi-Channel Adaptation Profile* (MCAP)
    - USB transport
      - *Universal Serial Bus Device Class Definition for Personal Healthcare Devices*
    - *ZigBee transpor*t
      - *ZigBee Health Profile Specification*
    - Near Field Communication (NFC) transport
      - *Personal Health Device Communication* (NFC Forum)
  - Bluetooth Low Energy
    - Bluetooth Low Energy Health Device Profiles and Services
    - *Personal Health Devices Transcoding White Paper*

For Bluetooth Low Energy (BTLE) the transcoding white paper maps PCHA compatible Bluetooth Low Energy attribute contents to IEEE 11073 20601 objects, attributes, and most importantly, nomenclature codes. The White Paper specifies a standardized means to translate BTLE data into IEEE 11073 data and thus PCD-01 OBX segments or FHIR resources. Only those BTLE devices that can map to the requirements of the white paper are compliant to the Communicate PCHA Data transaction.

3.15.4 Interaction Diagram

The Communicate PCHA Data transaction has two implementations, an IEEE 11073 20601 based packet exchange over any transport that is both reliable and delivers packets in order (currently four transports are recognized by PCHA), and an exchange using the Bluetooth Low Energy (BTLE) Generic Attribute (GATT) protocol. Both implementations first require the establishment of a connection. Once the connection is established, a series of exchanges take place that provide the Sensor Data Consumer with configuration and capability information about the Sensor Data Source. When the endpoints have completed this configuration, measurement data can be transferred.

The following interaction diagrams illustrate the sequence of processes for the IEEE and BTLE exchanges. When there are two flow illustrations in the figures, the IEEE exchange is to the left and the BTLE exchange is to the right. Figure 3.15.4-1 illustrates the sequence from connection establishment to data exchange exposing some of the details of the setup exchanges. Figures

3.15.4-2 and 3.15.4-3 illustrate the sequences for the data exchanges. Figure 3.15.4-2 illustrates the behavior when there is persistently stored data and Figure 3.15.4-3 illustrates the behavior for non-persistently stored data. It should be noted that a Sensor Data Source may have both types of data and the sequences illustrated in Figures 3.15.4-2 and 3.15.4-3 can happen simultaneously and/or in the same connection. Figure 3.15.4-4 summarizes the sequences into two groups: setup and data exchange. The triggering events, semantics, and expected actions for the summary sequence are then discussed in detail with references to the individual cases when needed.

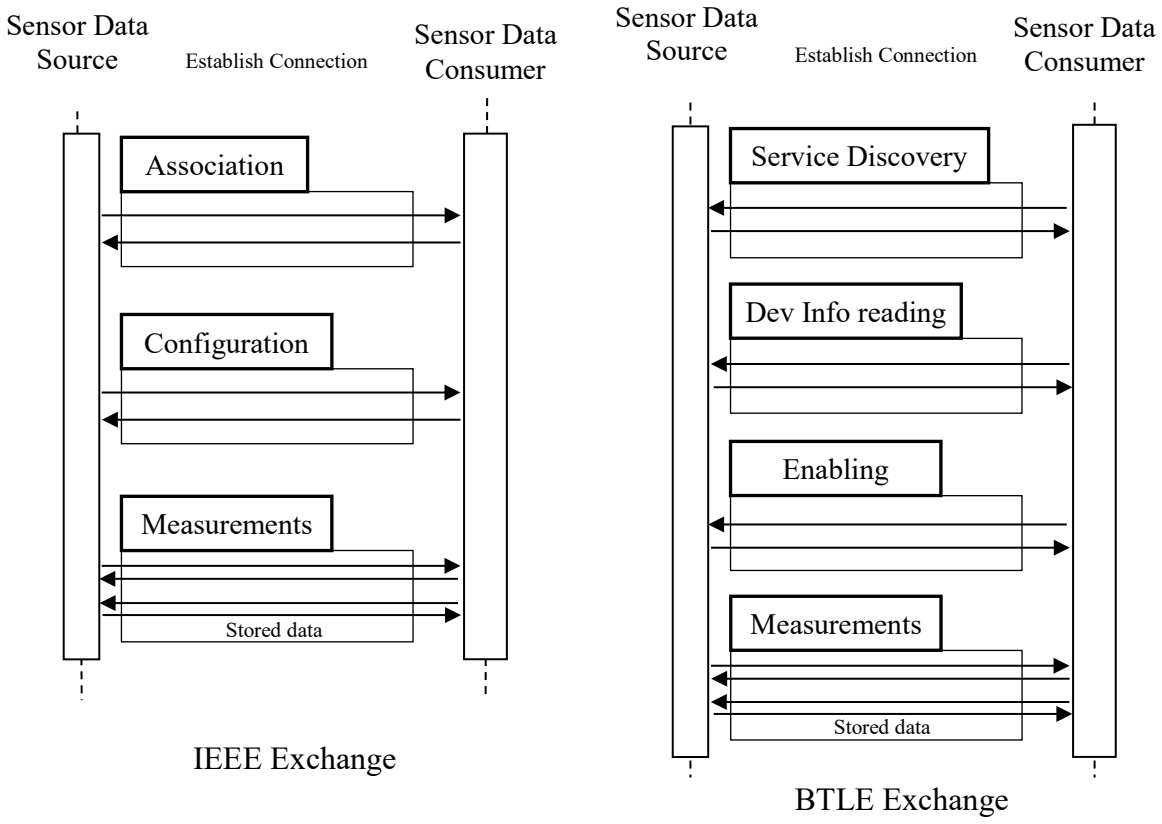


Figure 3.15.4-1: Complete PCHA Data Transaction

The above Figure illustrates the sequence of events that take place in the two different implementations of the PCHA transaction. In both cases, there is series of exchanges that allow the Sensor Data Consumer to either receive or request measurement data from the Sensor Data Source. It should be noted that the Sensor Data Consumer only requests data from the Sensor Data Source if the Sensor Data Source indicates that it has permanently stored data.

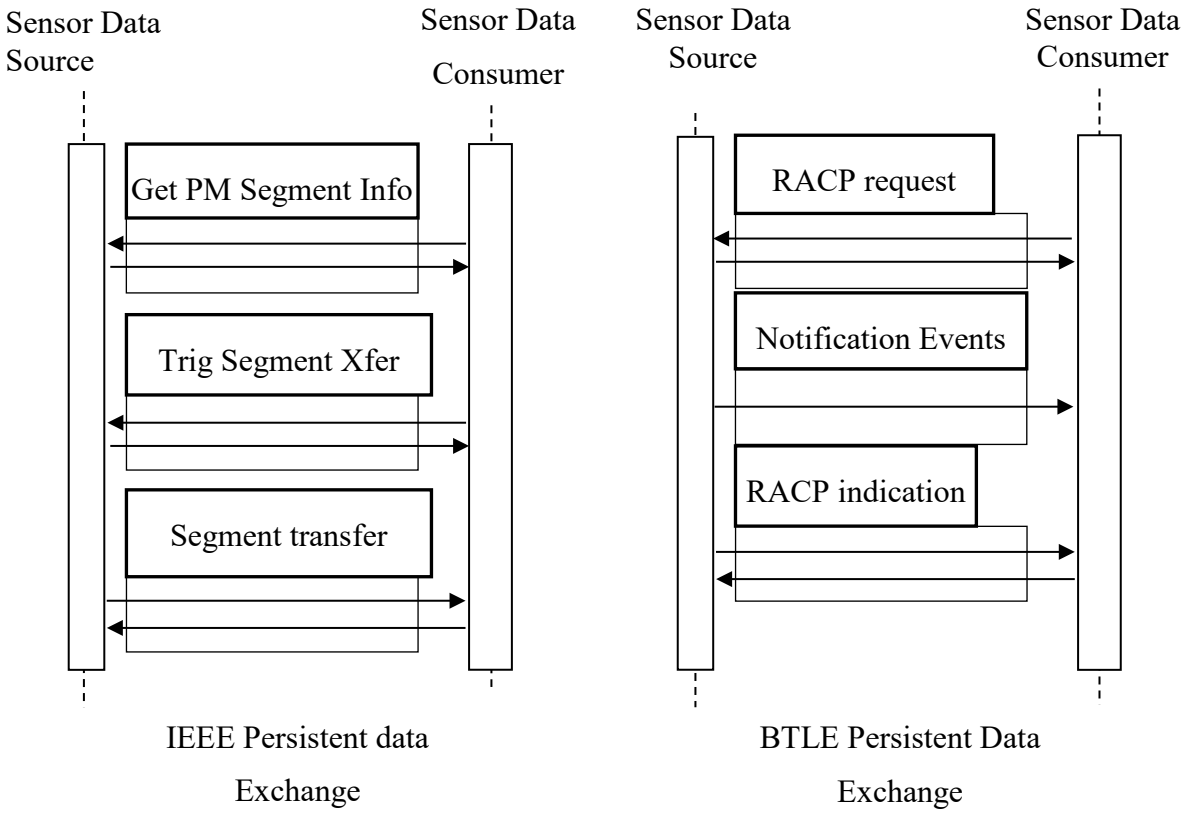


Figure 3.15.4-2: Persistent Data Exchanges

Figure 3.15.4-2 illustrates the exchanges for persistently stored data. In the IEEE case, the stored data is exposed as a set of Persistent Metric (PM) Stores (analogous to directories) containing PM Segments (analogous to files). Thus, the Sensor Data Consumer must query for the PM segments in the various PM Stores and then decide which PM Segment to transfer. It then requests the transfer of the given PM segment and the Sensor Data Source makes the transfer. In the BTLE case, there is but one 'file' but the Record Access Control Point (RACP) processes allow querying for its size as well as for transferring only parts of the entire data set. Once the RACP transfer is initiated the records are sent in notification events (they are NOT acknowledged). However, when the transfer is completed, an RACP indication (which IS acknowledged) indicates that the transfer is complete. Sequence numbers indicate to the Device Observation Consumer that all requested records have been received.

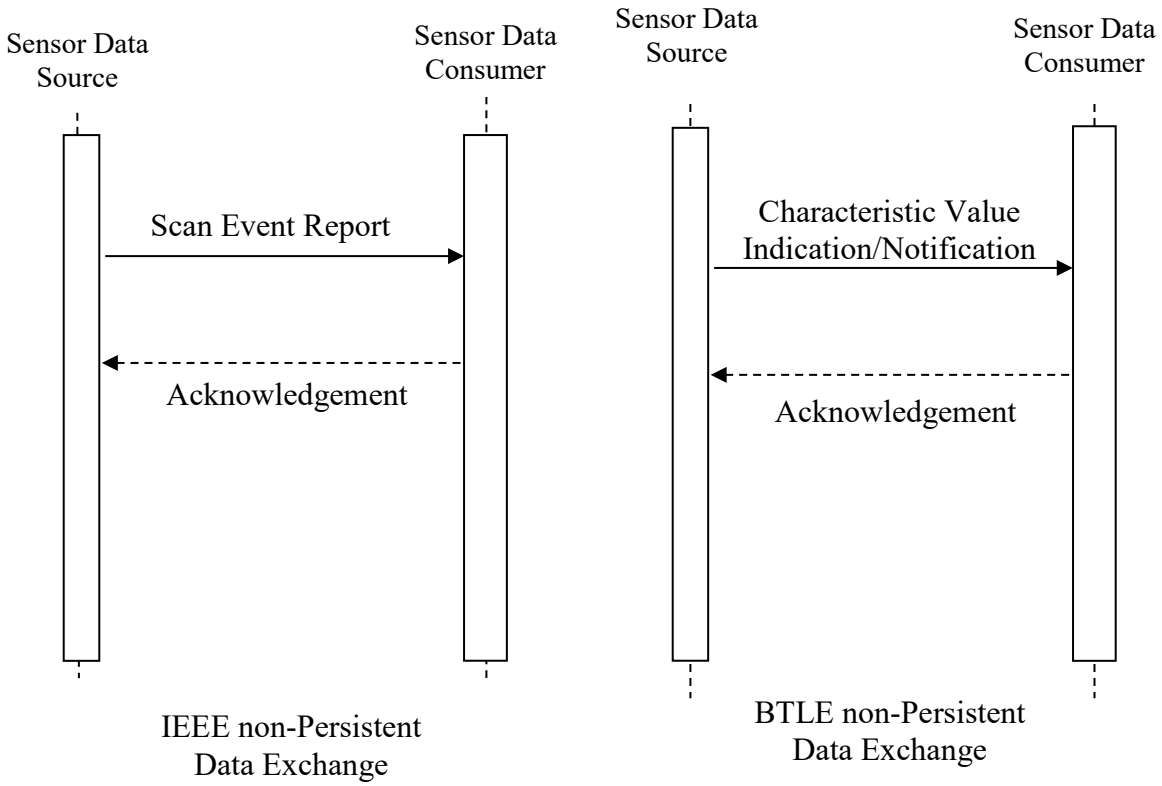


Figure 3.15.4-3: Non-Persistent Measurement Exchanges

Figure 3.15.4-3 illustrates the PCHA sequences for IEEE and BTLE when the Sensor Data Source and Sensor Data Consumer have been configured and there is non-persistent data to transfer. In this case, the Sensor Data Source sends the data unsolicited. Some transmissions are not acknowledged by the Sensor Data Consumer. Unacknowledged transmissions tend to be for streaming or waveform data.

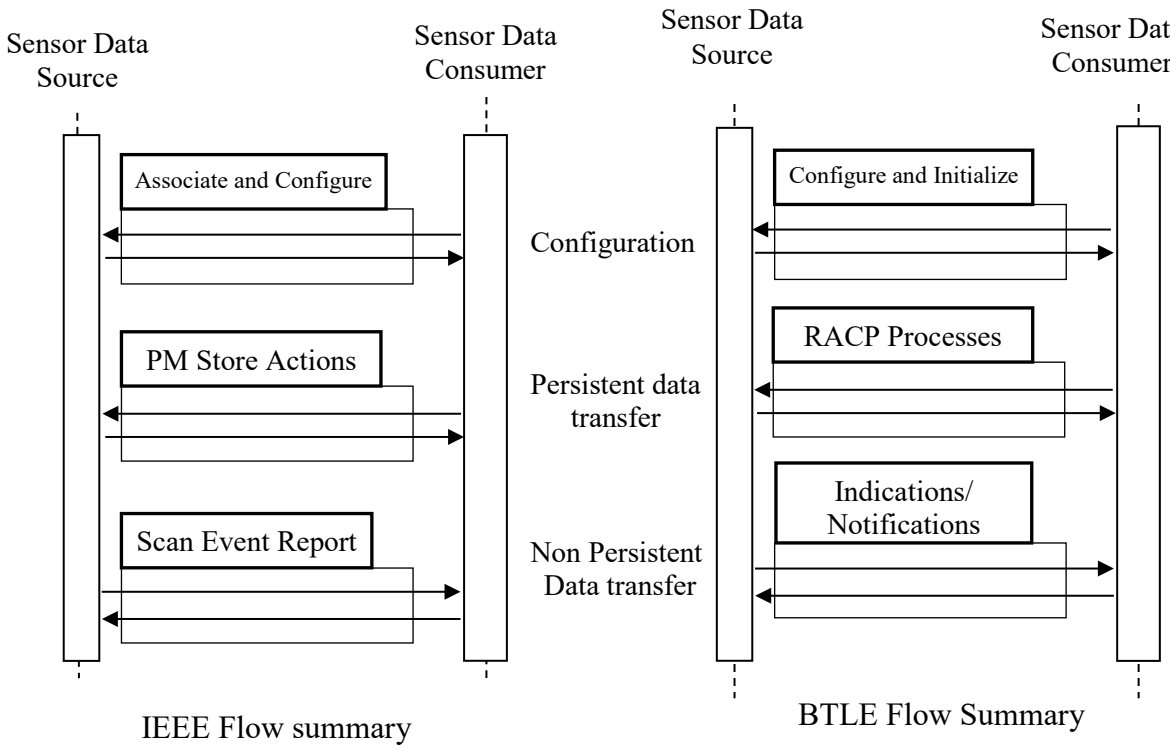


Figure 3.15.4-4: All Measurement Data Exchanges

Figure 3.15.4-4 summarizes the Communicate PCHA Data transaction for the IEEE and BTLE implementations. In both cases, there is a configuration stage preparing the actors for data transfer. And then in both cases there is a data transfer mechanism for persistent and non-persistent data. In both cases the Sensor Data Source sends non-persistent data unsolicited and in both cases the Sensor Data Consumer initiates the request for persistent data.

Minimal Sensor Data Consumer implementations are only required to support the transfer of non-persistent data. Persistent data is typically not invoked on a sensor device unless it is intended that more than 25 measurements are to be stored. Storing a limited number of measurements is called *temporarily stored data* in the IEEE protocol and is handled like non-persistent data. Weigh scales, pulse oximeters, thermometers, and blood pressure cuffs typically use temporarily stored data. Glucometers and continuous glucometers typically use persistently stored data.

3.15.4.1 Configuration

For all transports supported by the Communicate PCHA data transaction there is a configuration stage where the Sensor Data Consumer obtains information about the Sensor Data Source. This

information is necessary in order for the Sensor Data Consumer to receive and interpret the measurement data from the Sensor Data Source.

3.15.4.1.1 Trigger Events

The typical trigger events fall into two groups. The first is that the Sensor Data Source has measurement data to upload and the patient initiates the process for data upload. The second is that the patient is in the process of taking a measurement and a Sensor Data Consumer is either in range (wireless) or connected (wired) and active.

3.15.4.1.2 Message Semantics

In the IEEE implementation, the configuration messages consist of ASN.1 structures describing the IEEE 11073 20601 attributes present in the metric objects (measurements) the Sensor Data Source supports. There are also ASN.1 structures describing the Sensor Data Source properties (time capabilities, serial number, identifiers, etc.). ASN.1 structures are self-describing through the use of codes (or ids) and their TLV (Type, Length, Value) organization allows parse and ignore. These structures and their use in the objects, attributes, and APDUs are defined in Annex A of IEEE 11073 20601 Optimized Exchange Protocol. The major advantage of this protocol is that it is extensible. Since new specializations seldom define new ASN.1 structures, existing implementations are able to exchange data with, and decode data from, the new specializations without additional coding. Graphical displays will, however, need to provide human readable text for new nomenclature codes such as that code describing the new specialization; for example this is a continuous glucose monitoring device.

In the BTLE configuration the messages consist of GATT attributes to describe the services, characteristics, and descriptors on the Sensor Data Source. The services indicate what the Sensor Data Source supports, such as a thermometer service, heart rate service, blood pressure service, battery service, device information service, current time service, etc. If the right security has been established, the Sensor Data Consumer can read the characteristics in some of these services if it knows them and enable other characteristics to receive data. Every GATT service specifies its own set of characteristic and descriptors. They are unique and can only be decoded by knowing the specifications for the contained characteristic and descriptor attributes. Profile documents specify the services used by a given entity, for example the Glucose Profile specification. Separate service documents specify the characteristics and descriptors for the contained service(s) within a profile such as the Glucose Service and Device Information Service. The Bluetooth Special Interest Group maintains these documents. They also maintain a development portal at https://developer.bluetooth.org/Pages/default.aspx and specifically https://www.bluetooth.com/specifications/gatt where implementers can easily access the contents of these GATT attributes for all the currently defined services and profiles. Unlike the IEEE 11073 20601 specification which is extensible and new specializations require only the recognition of new nomenclature codes, new BTLE device profiles will require the addition of new GATT attributes and thus new profile and service specifications. Existing implementations will be unable to handle these new specifications.

3.15.4.1.3 Expected Actions

When the Sensor Data Source implements one or more of the PCHA BTLE Health Device Profiles then the initiation and configuration messages shall be performed using BTLE.

When the Sensor Data Source implements the PCHA IEEE 11073 20601 based option then the initiation and configuration messages shall be performed using IEEE 11073 20601 packets over one or more of USB, ZigBee, Bluetooth, or Near Field Communication (NFC) transport.

When the Sensor Data Consumer sends the confirmation to the Configuration sequence, the Sensor Data Consumer is expected to be ready to handle the reception of measurement data and the Sensor Data Source is expected to be ready to deliver measurement data.

3.15.4.2 Persistent Data Transfer

For the IEEE implementation, the Sensor Data Consumer uses the IEEE 11073 PM Store *actions* which are ASN.1 packets sent to the Sensor Data Source to query about and initiate the transfer of persistent data. For the BTLE implementation the Sensor Data Consumer uses the Record Access Control Point (RACP) processes which consist of writing to certain characteristics on the Sensor Data Source for the same purposes. This process is described in the Glucose Profile. For both implementations, the Sensor Data Source responds with the requested data transfer.

3.15.4.2.1 Trigger Events

This message is triggered by the existence of persistent data storage capabilities on the Sensor Data Source. The Sensor Data Consumer learns of these capabilities during configuration. Though most consumer implementations initiate the processes automatically, manual initiation is allowed.

3.15.4.2.2 Message Semantics

In the IEEE implementation, the actions initiated from the Sensor Data Consumer are ASN.1 structures indicating to the Sensor Data Source what to do. These instructions range from requesting information about the PM Segments (files) for a given PM Store (directory), beginning the transfer of a given PM Segment contained in a PM Store, to clearing one or more PM Segments contained in a PM Store. In the BTLE implementation the Sensor Data Consumer writes to RACP characteristics on the Sensor Data Source whose values indicate what to do. Similar to the IEEE implementation, the instructions request how much data is available, what data to transfer, and what data to clear.

In the IEEE implementation, the data is transferred in Segment Data Event packets and in the BTLE implementation the data is transferred in notification events. Sequence numbers keep track of the transfers and assure data consistency.

3.15.4.2.3 Expected Actions

Upon seeing that the Sensor Data Source has persistent storage capabilities, the Sensor Data Consumer is expected to query for the existence of any data and request the transfer of data it

wants. The Sensor Data Source is expected to provide the information and/or transfer the measurement data as instructed by the Sensor Data Consumer.

Deletion requests of the data by the Sensor Data Consumer are allowed. However, the Sensor Data Source is not required to support deletion and may refuse deletion in certain cases even though it supports the delete action.

When the Sensor Data Consumer acknowledges the receipt of this transfer it has taken responsibility for the data and passes it on to the Device Observation Reporter. The Sensor Data Source is now free to release any resources associated with the stored measurements.

3.15.4.3 Non-Persistent Data Transfer

In the IEEE implementation, non-persistent data is sent unsolicited in scan event report packets. Scan event reports contain ASN.1 Observation Scan structures that contain the updated components of the measurements. In the BTLE implementation non-persistent data is sent unsolicited in characteristic value change indication or notification events. The characteristic value may contain one or more different measurements.

3.15.4.3.1 Trigger Events

This message is triggered when the endpoints complete configuration and have data to send.

3.15.4.3.2 Message Semantics

In the IEEE implementation, the scan event report packets are ASN.1 structures containing the *changed* attributes of one or more metric objects (measurements) in ASN.1 Observation Scans. These changed attributes are combined with the unchanged attributes which have been mirrored on the Sensor Data Consumer to create the final completed measurements. In the BTLE implementation the indications or notifications typically contain one or more full measurements. Decoding is only possible if one knows the specification for the given characteristic.

3.15.4.3.3 Expected Actions

When the Sensor Data Consumer acknowledges the receipt of this message it has taken responsibility for the data and passes it on to the Device Observation Reporter. The Sensor Data Source is now free to release any resources associated with the measurement.

3.15.5 Security Considerations

The Communicate PCHA Data transaction is local; that is the Sensor Data Source is expected to be in the proximity of the Sensor Data Consumer. In the case of wired transports (USB), the security risks in the exchange are considered to be so low the data is transferred without any encryption. However, unencrypted wireless transports could be intercepted and modified by a malicious third party and the PCHA transaction requires the use of the available encryption options in the wireless protocols.

3.15.5.1 Security Audit Considerations

There are no auditing requirements in these transactions.

3.15.5.1.1 Sensor Data Source Specific Security Considerations

The primary security risk facing the Sensor Data Source is the compromising of personal health data via theft of the device. This risk is, in practice, quite low since the Sensor Data Source rarely contains any personal information since the transport protocols of the Communicate PCHA Data transaction do not support the transmission of personal data to the Sensor Data Consumer. The Communicate PCHA Data transaction also does not currently support control and or configuration of the Sensor Data Source from the Sensor Data Consumer thus the threat of malicious configuration of the device is low. However, there are current developments in the Communicate PCHA Data transaction for the configuration/control of the Sensor Data Source from the Sensor Data Consumer. That option will demand additional security considerations that have not yet been worked out.

3.15.5.1.2 Sensor Data Consumer Specific Security Considerations

The greatest security risk facing the Sensor Data Consumer is the compromising of personal data via theft of the device. Unlike the Sensor Data Source, the Sensor Data Consumer is often a personal mobile device such as an Android phone or tablet and these devices may have all kinds of personal information; including financial. The Sensor Data Consumer implementation may also store the medical data for review. What the Sensor Data Consumer does with the received data beyond passing the data to the Device Observation Reporter or Content Creator is not specified by the Communicate PCHA Data transactions. Local storage of the data and whether or not it is encrypted is application dependent.

3.21 PCD Communicate PCD Data-hData Transaction [PCC-21]

3.21.1 Scope

These transactions are used to transfer collected patient measurement data to a Device Observation Consumer in the form of a PCD-01 message

3.21.2 Actor Roles

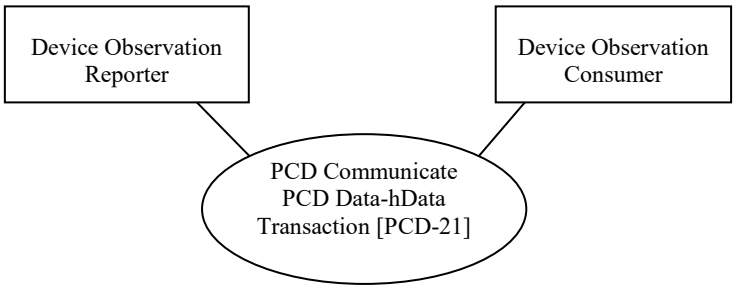


Figure 3.21.2-1: Use Case Diagram

Table 3.21.2-1: Actor Roles

Actor:	Device Observation Reporter
Role:	This actor is responsible for packaging patient measurement data into a PCD-01 message and sending it to a Device Observation Consumer
Actor:	Device Observation Consumer
Role:	This actor receives the PCD-01 message from one or more Device Observation Reporters

Since the Device Observation Reporter does not receive any patient demographic information from the PHD device, at least the patient name, a patient identifier and authorization code are required to create a compliant PID segment for the PCD-01 message. The Device Observation Reporter implementation will be required to provide this supplemental information, and when appropriate, map it to the optional person-id that is sometimes provided by PHD devices. A Device Observation Reporter implementation may also provide a filter such that only certain measurements are forwarded in the PCD-01 message. Such a filter is implementation dependent and outside the scope of this profile, but clearly the filter must still generate a compliant PCD-01 message.

3.21.3 Referenced Standards

The PCD Communicate PCD data-hData transaction is specified in the PCHA H.812.1 – Observation Upload, PCHA H.812 WAN IF Common Certified Device Class Guidelines, and PCHA H.812.3 Capability Exchange documents. The hData record format is specified in HL7 Version 3 Standard: hData Record Format Release, 1. Authentication is further specified in IHE Technical Framework Supplement: Internet User Authentication.

3.21.4 Interaction Diagram

The diagram below illustrates the Communicate PCD Data-hData transaction. How one obtains the authentication token is not specified by this profile.

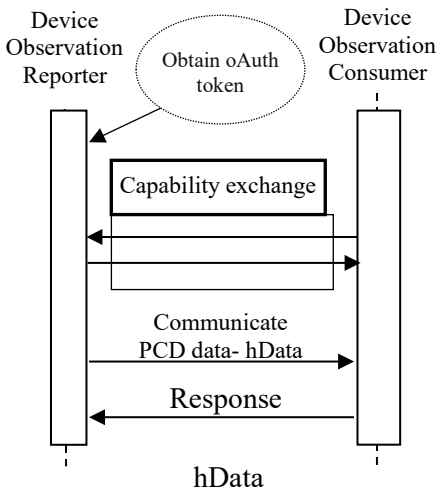


Figure 3.21.4-1: Communication PCD Data-hData Transaction

3.21.4.1 Capability Exchange

The Capability exchange encapsulates the first stage of all hData transactions which consist of obtaining the root.xml. This file provides the Device Observation Reporter with the features and resource directory of the Device Observation Consumer in a standardized manner.

3.21.4.1.1 Trigger Events

The typical trigger event is initialization of communications between the Device Observation Reporter and Device Observation Consumer. This initialization may not happen until the Device Observation Reporter is passed measurement data.

3.21.4.1.2 Message Semantics

In RESTful POST transactions the root.xml file is obtained using an HTTP GET on the base URL. The base URL is obtained by an out-of-band means. The root.xml is to hData what the WSDL is to Web Services. The request for the root.xml is the first action all hData clients take in order to interoperate with an hData server. The PCHA H 812.3 Capability Exchange utilizes the profile, section, representation, and resourceType elements of the hData record format to specify what PCHA certified device classes are supported by the Device Observation Consumer as well as the information needed by the client to interoperate with these certified device classes. The hData Observation-upload is one of the certified device classes that shall be described in the root.xml if the endpoint supports the transaction. Figures 7-2 to 7-5 in the PCHA H 812.1 Observation Upload specification show examples of the capability elements as they might appear for a Device Observation Consumer that supports (1) observation upload by hData, (2) observation upload by SOAP web services, (3) an STS SAML Token server, and (4) an oAuth 2.0 authentication service. Only the observation upload by hData capability is required for hData

servers that support that capability, since the web services capabilities are not RESTful and web service clients will not be expected to access and understand hData root.xmls. However, specifying the web services capabilities in the exchange can make for a more user friendly experience on dual capability clients.

For the Communicate PCD Data hData transaction, the Capability Exchange Profile/path element provides the Device Observation Reporter with the URL for the HTTP POST of the PCD-01 message. The Capability Exchange in general also provides the location of any schemas, the form of the document (xml, text, etc.), and the document specifying the standard for the transaction. Extension elements can be used to provide additional information.

3.21.4.1.3 Expected Actions

The handling of this message is primarily internal and no expected actions result. However, the obtained information is essential in order for the Device Observation Reporter to invoke the RESTful Communicate PCD Data-hData transaction.

3.21.4.2 Communicate PCD Data-hData

The Communicate PCD Data-hData transaction used in this profile uses RESTful HL7 hData Record Format specified in HL7 Version 3 Standards: Record Data Format Release 1 to transfer the PCD-01 message to the Device Observation Consumer. The PCHA H.812.1 Observation upload specification requires that the Device Observation Consumer and Device Observation Reporter Actors support TLS security and oAuth authentication on the hData transport. ATNA auditing is an option.

It is this component of the message that transfers the measurement data as a PCD-01 message to the Device Observation Consumer. The security and authentication requirements are present since this transaction is not locally bound like the Communicate PCHA Data transaction and in this profile it is the transaction responsible for transferring the medical data from the remote location of the patient to an enterprise or third party server which can be located anywhere there is connectivity. Typically this would be the internet and it could occur from an unsecured public network.

Full on-the-wire examples of the hData transaction including the request for the oAuth token is given in PCHA H 812.1 Observation Upload section 8.11. The example is repeated with the capability exchange in Appendix J. The PCHA H 812.1 Observation Upload specification also provides a detailed description of how to map IEEE 11073 20601 metric object attributes to PCD-01 MDS and Metric OBX segments in Annex D.0 – D.1.4. Given the Bluetooth Low Energy Transcoding White Paper the same mapping descriptions can be used for PCHA-compliant Bluetooth Low Energy devices. In addition to the generic mapping description, the PCHA H 812.1 Observation Upload has a set of tables that map the IEEE 11073 20601 device specialization attributes to metric OBX segments in Annex E.

3.21.4.2.1 Trigger Events

The typical trigger event is the passing of a collection of measurement data to the Device Observation Reporter.

3.21.4.2.2 Message Semantics

The RESTful transport implementation of this message contains both an oAuth identity token and the PCD-01 message which represents the measurement sequence taken upon the patient. The message consists of a simple HTTP POST containing the oAuth token to the URL specified by the Device Observation Consumer in its root.mxl obtained during Capability Exchange. The body of the message is the PCD-01 message. The oAuth identity token must be recognized by the Device Observation Consumer for acceptance of the message but how that identity token is obtained is a business trust relationship decision. The Device Observation Consumer may be an oAuth Authentication Server, or the Device Observation Reporter may obtain the token from a third party service trusted by the Device Observation Consumer, or the token may be obtained by an out of band means.

This message also represents an attempt to pass responsibility of the data from the Device Observation Reporter to the Device Observation Consumer.

3.21.4.2.3 Expected Actions

The expected behavior by the Device Observation Consumer upon reception of this message is to first authenticate the identity of the sender and if authenticated to transfer the PCD-01 message to the Content Creator. The Device Observation Consumer is then expected to indicate to the Device Observation Reporter whether or not the transfer is successful by responding with an appropriate acknowledgement.

3.21.4.3 Acknowledgement

The Acknowledgement is a response to the Communicate PCD Data-hData message and indicates the status of the transaction. The consequence of this message indicates whether or not responsibility for the data is transferred from the Device Observation Reporter to the Device Observation Consumer.

3.21.4.3.1 Trigger Events

The Acknowledgement is triggered by the reception of the Communicate PCD Data-hData at the Device Observation Consumer.

3.21.4.3.2 Message Semantics

This message consists of an HTTP response indicating the status of the transaction plus a PCD-01 response message as defined in IHE PCD-TF Vol 2 Transactions. The PCD-01 response consists of up to three segments where the ERR segment is optional. In spite of its name, the ERR segment may also be present when the received PCD-01 message is handled successfully. The ERR segment provides a field ERR-6 that may contain any additional information the server wishes to add. ERR-1 and/or ERR-2 provide error codes, and one of the codes indicates success. The server could indicate to the client that the PCD-01 message was successfully archived or successfully converted to a PHMR and transferred to its final repository.

3.21.4.3.3 Expected Actions

Upon a successful transaction the Device Observation Reporter is free to release any resources associated with the measurement data. The Device Observation Consumer is expected to transfer the data to the Content Creator.

3.21.5 Security Considerations

The Communicate PCD Data-hData transaction is subject to any of the security threats of transactions that utilize the public internet and unsecure public networks. To assure some level of consistent security, this transaction requires, at minimum, support for TLS encryption and the support of oAuth BearerToken authentication in this transaction.

3.21.5.1 Security Audit Considerations

There are no auditing requirements in this transaction though the use of ATNA auditing is optional.

3.21.5.2 Device Observation Reporter Specific Security Considerations

Being part of the Sensor Data Consumer or Sensor Data Source, the Device Observation Reporter faces the same security risks as those actors; the primary risk being compromising of personal data via theft of the device. The Device Observation Reporter is often a personal mobile device such as an Android phone or tablet and these devices may have all kinds of personal information; including financial. The Device Observation Reporter implementation will store medical data on failed transfers and it may also store the medical data for review. Since the unit is often in the home, it may fall outside of any regional safeguards that might be in place for health care providers and associated supporting partners that will handle personal medical data. On the other hand, given that the range of data sensitivity in a remote patient monitoring situation is so great, no non-transaction based security requirements are required. Encryption of local data, and password, fingerprint, facial recognition, etc. access to the unit hosting the Device Observation Reporter software is left up to the implementation.

3.21.5.3 Device Observation Consumer Specific Security Considerations

The Device Observation Consumer is typically resident on a third party remote server or a server located at the institution of the health care provider. This actor has all the security risks that any medical data stored in a professional environment faces. It is likely subject to regional safeguards for the handling of personal medical data.

3.22 PCD Communicate PCD Data-SOAP Transaction [PCC-22]

3.22.1 Scope

This transaction is used to transfer collected patient measurement data to a Device Observation Consumer in the form of a PCD-01 message using secured Web Services CommunicatePCDData SOAP action authenticated by SAML.

3.22.2 Actor Roles

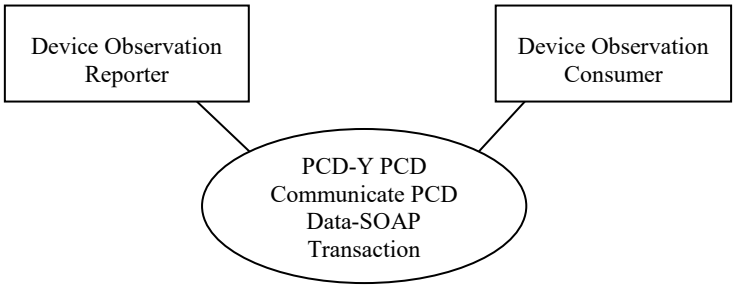


Figure 3.22.2-1: Use Case Diagram

Table 3.22.2-1: Actor Roles

Actor:	Device Observation Reporter
Role:	This actor is responsible for packaging patient measurement data into a PCD-01 message and sending it to a Device Observation Consumer
Actor:	Device Observation Consumer
Role:	This actor receives the PCD-01 message from one or more Device Observation Reporters

Since the Device Observation Reporter does not receive any patient demographic information from the PHD device; at least the patient name, a patient identifier and authorization code are required to create a compliant PID segment for the PCD-01 message. The Device Observation Reporter implementation will be required to provide this supplemental information, and when appropriate, map it to the optional person-id that is sometimes provided by PHD devices. A Device Observation Reporter implementation may also provide a filter such that only certain measurements are forwarded in the PCD-01 message. Such a filter is implementation dependent and outside the scope of this profile, but clearly the filter must still generate a compliant PCD-01 message.

3.22.3 Referenced Standards

The PCD Communicate PCD data-SOAP transaction is specified in the PCHA H.812.1 Observation Upload specification which references the CommunicatePCDData SOAP action in PCD TF-Vol 1-3.0, PCD TF-Vol 2-3.0, and PCD TF-Vol 3-3.0.

3.22.4 Interaction Diagram

The figure below illustrates the Communicate PCD Data-SOAP transaction. The transaction requires an out-of-band action to obtain a SAML2.0 authentication token.

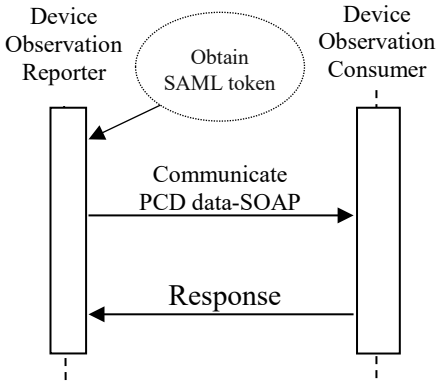


Figure 3.22.4-1: Communication PCD-Data – SOAP Transaction

3.22.4.1 Communicate PCD Data-SOAP

The Communicate PCD Data-SOAP transaction transfers a PCD-01 message in a CommunicatePDCData SOAP action over web services. This transport is specified in the PCD TF-1to3. The PCHA H.812.1 Observation upload specification requires that the Device Observation Consumer supports TLS security, SAML 2.0 authentication, and WS reliable messaging on this web services transport. The same requirements are placed upon the Device Observation Reporter except that Reliable messaging is optional. ATNA auditing is an option.

It is this component of the message that transfers the measurement data as a PCD-01 message to the Device Observation Consumer. The security and authentication requirements are present since this transaction is not locally bound like the Communicate PCHA Data transaction and in the RPM Profile it is the transaction responsible for transferring the medical data from the remote location of the patient to an enterprise or third party server which can be located anywhere there is connectivity. Typically, this would be the internet and the transaction could take place from exposed public networks.

Full on-the-wire examples of the SOAP transaction including requests for the SAML token is given in PCHA H 812.1 Observation Upload sections 8.10. The example is repeated in Appendix K. The PCHA H 812.1 Observation Upload specification also provides a detailed description of how to map IEEE 11073 20601 metric object attributes to PCD-01 MDS and Metric OBX segments in Annex D.0 – D.1.4. Given the Bluetooth Low Energy Transcoding White Paper the same mapping descriptions can be used for PCHA-compliant Bluetooth Low Energy devices. In addition to the generic mapping description, the PCHA H 812.1 Observation Upload has a set of tables that map the IEEE 11073 20601 device specialization attributes to metric OBX segments in Annex E.

3.22.4.1.2 Trigger Events

The typical trigger event is the passing of a collection of measurement data to the Device Observation Reporter.

3.22.4.1.3 Message Semantics

The transport implementation of this message contains both a SAML2.0 identity token and the PCD-01 message which represents the measurement sequence taken upon the patient. The PCD-01 message is encapsulated in a CommunicatePCDData SOAP action. WS-Addressing and WS-Security elements housing the SAML2.0 token are present in the SOAP header. The SAML identity token must be recognized and validated by the Device Observation Consumer for acceptance of the message but how that identity token is obtained is a business trust relationship decision. The Device Observation Consumer may be a SAML token Server, or the Device Observation Consumer may rely upon a third party service to provide the token to the Device Observation Reporter, or the Device Observation Reporter may obtain the token by another out of band means.

This transaction also represents an attempt to pass responsibility of the data from the Device Observation Reporter to the Device Observation Consumer.

3.22.4.1.4 Expected Actions

The expected behavior by the Device Observation Consumer upon reception of this message is to first authenticate the identity of the sender and if authenticated to transfer the PCD-01 message to the Content Creator. The Device Observation Consumer is then expected to indicate to the Device Observation Reporter whether or not the transfer is successful by responding with an appropriate acknowledgement.

3.22.4.2 Acknowledgement

The Acknowledgement is a response to the Communicate PCD Data-SOAP message and indicates the status of the transaction. The consequence of this message indicates whether or not responsibility for the data is transferred from the Device Observation Reporter to the Device Observation Consumer.

3.22.4.2.1 Trigger Events

The Acknowledgement is triggered by the reception of the Communicate PCD Data-SOAP transaction at the Device Observation Consumer.

3.22.4.2.2 Message Semantics

This message consists of Web services WS-Addressing and WS_Security header with a CommunicatePCDDataResponse SOAP action containing a PCD-01 response message as defined in IHE PCD-TF Vol 2 Transactions. The PCD-01 response consists of up to three segments where the ERR segment is optional. In spite of its name, the ERR segment may also be present when the received PCD-01 message is handled successfully. The ERR segment provides

a field ERR-6 that may contain any additional information the server wishes to add. ERR-1 and/or ERR-2 provide error codes, and one of the codes indicates success. The server could indicate to the client that the PCD-01 message was successfully archived or successfully converted to a PHMR and transferred to its final repository.

3.22.4.2.3 Expected Actions

Upon a successful transaction the Device Observation Reporter is free to release any resources associated with the measurement data. The Device Observation Consumer is expected to transfer the data to the Content Creator.

3.22.5 Security Considerations

The Communicate PCD Data-SOAP transaction, like the Communicate PCD Data-hData transaction is subject to any of the security threats of transactions that utilize the public internet and unsecure public networks. To assure some level of consistent security, this transaction requires, at minimum, support for TLS encryption and the support of SAML authentication in this transaction. Additional security restrictions such as message level security are optional and are determined by business needs.

3.22.5.1 Security Audit Considerations

There are no auditing requirements in this transaction though the use of ATNA auditing is optional.

3.22.5.2 Device Observation Reporter Specific Security Considerations

Being part of the Sensor Data Consumer or Sensor Data Source, the Device Observation Reporter faces the same security risks as those actors; the primary risk being compromising of personal data via theft of the device. The Device Observation Reporter is often a personal mobile device such as an Android phone or tablet and these devices may have all kinds of personal information; including financial. The Device Observation Reporter implementation will store medical data on failed transfers and it may also store the medical data for review. Since the unit is often in the home, it may fall outside of any regional safeguards that might be in place for health care providers and associated supporting partners that will handle personal medical data. On the other hand, given that the range of data sensitivity in a remote patient monitoring situation is so great, no non-transaction based security requirements are required. Encryption of local data, and password, fingerprint, facial recognition, etc. access to the unit hosting the Device Observation Reporter software is left up to the implementation.

3.22.5.3 Device Observation Consumer Specific Security Considerations

The Device Observation Consumer is typically resident on a third party remote server or a server located at the institution of the health care provider. This actor has all the security risks that any medical data stored in a professional environment faces. It is likely subject to regional safeguards for the handling of personal medical data.

3.42 Communicate FHIR Data-hData Transaction [PCC-42]

3.42.1 Scope

These transactions are used to transfer collected patient measurement data to a Device Observation Consumer in the form of a complete FHIR Bundle.

3.42.2 Actor Roles

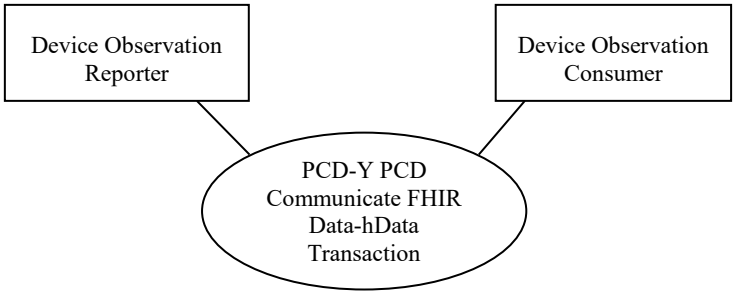


Figure 3.42.2-1: Use Case Diagram

Table 3.42.2-1: Actor Roles

Actor:	Device Observation Reporter
Role:	This actor is responsible for packaging patient measurement data into a complete FHIR Bundle and sending it to a Device Observation Consumer
Actor:	Device Observation Consumer
Role:	This actor receives the FHIR Bundle from one or more Device Observation Reporters

Since the Device Observation Reporter does not receive any patient demographic information from the PHD device, at least the patient name, a patient identifier and authorization code are required to create a compliant Patient resource. The Device Observation Reporter implementation will be required to provide this supplemental information, and when appropriate, map it to the optional person-id that is sometimes provided by PHD devices. A Device Observation Reporter implementation may also provide a filter such that only certain measurements are forwarded in the FHIR Bundle. Such a filter is implementation dependent and outside the scope of this profile, but clearly the filter must still generate a compliant FHIR Bundle.

3.42.3 Referenced Standards

The Communicate FHIR data-hData transaction is specified in the PCHA H.812.5 – FHIR Upload, PCHA H.812 WAN IF Common Certified Device Class Guidelines, and PCHA H.812.3 Capability Exchange documents. The hData record format is specified in HL7 Version 3

Standard: hData Record Format Release, 1 though the only aspect of the RESTful function is the create action. Authentication is further specified in IHE Technical Framework Supplement: Internet User Authentication.

3.42.4 Interaction Diagram

The diagram below illustrates the Communicate FHIR Data-hData transaction. How one obtains the authentication token is not specified by this profile.

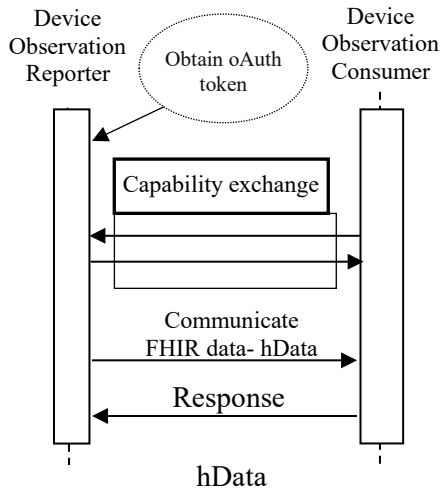


Figure 3.42.4-1: Communication FHIR Data-hData Transaction

3.42.4.1 Capability Exchange

The Capability exchange encapsulates the first stage of all hData transactions which consist of obtaining the root.xml. This file provides the Device Observation Reporter with the features and resource directory of the Device Observation Consumer in a standardized manner.

3.42.4.1.1 Trigger Events

The typical trigger event is initialization of communications between the Device Observation Reporter and Device Observation Consumer. This initialization may not happen until the Device Observation Reporter is passed measurement data.

3.42.4.1.2 Message Semantics

In RESTful POST transactions the root.xml file is obtained using an HTTP GET on the base URL. The base URL is obtained by an out-of-band means. The root.xml is to hData what the WSDL is to Web Services. The request for the root.xml is the first action all hData clients take in order to interoperate with an hData server. The PCHA H 812.3 Capability Exchange utilizes the profile, section, representation, and resourceType elements of the hData record format to specify

what PCHA certified device classes are supported by the Device Observation Consumer as well as the information needed by the client to interoperate with these certified device classes. The hData Observation-upload is one of the certified device classes that shall be described in the root.xml if the endpoint supports the transaction. Figures 7-2 to 7-5 in the PCHA H 812.1 Observation Upload specification show examples of the capability elements as they might appear for a Device Observation Consumer that supports (1) observation upload by hData, (2) observation upload by SOAP web services, (3) an STS SAML Token server, and (4) an oAuth 2.0 authentication service. Only the observation upload by hData capability is required for hData servers that support that capability, since the web services capabilities are not RESTful based and web service clients will not be expected to access and understand hData root.xmls. However specifying the web services capabilities in the exchange can make for a more user friendly experience on multiple capability clients.

For the Communicate FHIR Data hData transaction, the Capability Exchange Profile/path element provides the Device Observation Reporter with the URL for the HTTP POST of the FHIR Bundle. The Capability Exchange in general also provides the location of any schemas, the form of the document (json, xml, etc.), and the document specifying the standard for the transaction. Extension elements can be used to provide additional information.

3.42.4.1.3 Expected Actions

The handling of this message is primarily internal and no expected actions result. However, the obtained information is essential in order for the Device Observation Reporter to invoke the RESTful Communicate FHIR Data-hData transaction.

3.42.4.2 Communicate FHIR Data-hData

The Communicate FHIR Data-hData transaction used in this profile uses RESTful HL7 hData Record Format specified in HL7 Version 3 Standards: Record Data Format Release 1 to transfer the FHIR Bundle to the Device Observation Consumer, but only with respect to the upload. The PCHA H.812.5 Observation upload specification requires that the Device Observation Consumer and Device Observation Reporter Actors support TLS security and oAuth authentication on the hData transport. ATNA auditing is an option.

It is this component of the message that transfers the measurement data as a FHIR Bundle to the Device Observation Consumer. The security and authentication requirements are present since this transaction is not locally bound like the Communicate PCHA Data transaction and in the RPM Profile it is the transaction responsible for transferring the medical data from the remote location of the patient to an enterprise or third party server which can be located anywhere there is connectivity. Typically, this would be the internet and it could occur from an unsecured public network.

Full on-the-wire examples of the hData transaction including the request for the oAuth token is given in PCHA H 812.1 Observation Upload section 8.11 though the data contained is a PCD-01 message and not a FHIR Bundle. The example is repeated with the capability exchange in Appendix J. The PCHA H 812.5 FHIR Upload specification also provides a detailed description of how to map IEEE 11073 20601 metric object attributes to FHIR Device, DeviceComponent,

DeviceMetric, and Observation resources. Given the Bluetooth Low Energy Transcoding White Paper the same mapping descriptions can be used for PCHA-compliant Bluetooth Low Energy devices.

3.42.4.2.1 Trigger Events

The typical trigger event is the passing of a collection of measurement data to the Device Observation Reporter.

3.42.4.2.2 Message Semantics

The RESTful transport implementation of this message contains both an oAuth identity token and the FHIR Bundle which represents the measurement sequence taken upon the patient. The message consists of a simple HTTP POST containing the oAuth token to the URL specified by the Device Observation Consumer in its root.mxl obtained during Capability Exchange. The body of the message is the FHIR Bundle. The oAuth identity token must be recognized by the Device Observation Consumer for acceptance of the message but how that identity token is obtained is a business trust relationship decision. The Device Observation Consumer may be an oAuth Authentication Server, or the Device Observation Reporter may obtain the token from a third party service trusted by the Device Observation Consumer, or the token may be obtained by an out of band means.

This message also represents an attempt to pass responsibility of the data from the Device Observation Reporter to the Device Observation Consumer. Once received, there is no further responsibility of the Device Observation Consumer to persist the uploaded resource.

3.42.4.2.3 Expected Actions

The expected behavior by the Device Observation Consumer upon reception of this message is to first authenticate the identity of the sender and if authenticated to transfer the FHIR Bundle to the Content Creator. The Device Observation Consumer is then expected to indicate to the Device Observation Reporter whether or not the transfer is successful by responding with an appropriate acknowledgement.

3.42.4.3 Acknowledgement

The Acknowledgement is a response to the Communicate FHIR Data-hData message and indicates the status of the transaction. The consequence of this message indicates whether or not responsibility for the data is transferred from the Device Observation Reporter to the Device Observation Consumer.

3.42.4.3.1 Trigger Events

The Acknowledgement is triggered by the reception of the Communicate FHIRD Data-hData at the Device Observation Consumer.

3.42.4.3.2 Message Semantics

This message consists of an HTTP response indicating the status of the transaction.

3.42.4.3.3 Expected Actions

Upon a successful transaction, the Device Observation Reporter is free to release any resources associated with the measurement data. The Device Observation Consumer is expected to transfer the data to the Content Creator.

3.42.5 Security Considerations

The Communicate FHIR Data-hData transaction is subject to any of the security threats of transactions that utilize the public internet and unsecure public networks. To assure some level of consistent security, this transaction requires, at minimum, support for TLS encryption and the support of oAuth BearerToken authentication in this transaction.

3.42.5.1 Security Audit Considerations

There are no auditing requirements in this transaction though the use of ATNA auditing is optional.

3.42.5.2 Device Observation Reporter Specific Security Considerations

Being part of the Sensor Data Consumer or Sensor Data Source, the Device Observation Reporter faces the same security risks as those actors; the primary risk being compromising of personal data via theft of the device. The Device Observation Reporter is often a personal mobile device such as an Android phone or tablet and these devices may have all kinds of personal information; including financial. The Device Observation Reporter implementation will store medical data on failed transfers and it may also store the medical data for review. Since the unit is often in the home, it may fall outside of any regional safeguards that might be in place for health care providers and associated supporting partners that will handle personal medical data. On the other hand, given that the range of data sensitivity in a remote patient monitoring situation is so great, no non-transaction based security requirements are required. Encryption of local data, and password, fingerprint, facial recognition, etc. access to the unit hosting the Device Observation Reporter software is left up to the implementation.

3.42.5.3 Device Observation Consumer Specific Security Considerations

The Device Observation Consumer is typically resident on a third party remote server or a server located at the institution of the health care provider. This actor has all the security risks that any medical data stored in a professional environment faces. It is likely subject to regional safeguards for the handling of personal medical data.

Appendices

None

Volume 2 Namespace Additions

Add the following terms to the IHE General Introduction Appendix G:

None

Volume 3 – Content Modules

5 Namespaces and Vocabularies

Add to Section 5 Namespaces and Vocabularies

1505

codeSystem	codeSystemName	Description
2.16.840.1.113883.6.24	ISO/IEEE 11073-10101 Medical Device Communication Nomenclature	See http://www.hl7.org/oid/index.cfm?Comp_OID=2.16.840.1.113883.6.24 for more details.

Add to Section 5.1.1 IHE Format Codes

Profile	Format Code	Media Type	Template ID
Personal Health Monitoring Report (PHMR)	urn:ihe:pcc:phmr:2015	Text/xml	TBD

6 Content Modules

6.3.1 CDA®[3] Document Content Modules

Add to Section 6.3.1.D CDA Document Content Modules

6.3.1.D Personal Healthcare Monitoring Report (PHMR) Document Content Module

6.3.1.D.1 Format Code

The XDSDocumentEntry format code for this content is **urn:ihe:pcc:phmr:2015**

6.3.1.D.2 Parent Template

This document is a specialization of the IHE PCC Medical Document template (OID = 1.3.6.1.4.1.19376.1.5.3.1.1.1).

6.3.1.D.3 Referenced Standards

All standards which are reference in this document are listed below with their common abbreviation, full title, and link to the standard.

Table 6.3.1.D.3-1: PHMR - Referenced Standards

Abbreviation	Title	URL
PHMR	Personal Health Monitoring Report	TBD
C-CDA	HL7 Clinical Document Architecture	TBD

6.6 FHIR Resource Content Modules

Add to Section 6.6.x FHIR Resource Content Modules

The word ‘profile’ is overloaded. Thus this document will specifically indicate which use is being referenced; such as IHE profile or FHIR profile.

The FHIR resource Content Creator requires the use of the Patient, Device, DeviceComponent, DeviceMetric, and Observation resources. The information that is required to be entered into the profiled resources, except the Patient resource, comes from the PHD via the 11073-20601

[3] CDA is the registered trademark of Health Level Seven International.

exchange protocol or mapped equivalent; no additional entry by the user of the PHD is required. The set of required resources and FHIR-profiled elements in these resources are unchanged on the wire in both DSTU2 and STU3 versions of the specification with the exception of the DeviceComponent.lastSystemChange. It is optional in STU3 3.0.0 but is required in previous versions. This value is not obtainable by protocol and in versions of FHIR previous to STU3 3.0.0 it is set to a fixed value of January 1, 1970, 00:00:00 (the Unix time stamp 0). In STU3 3.0.0 the DeviceComponent.lastSystemChange element may be omitted. In this manner, the RPM FHIR Content Creator can interoperate with FHIR Content Consumers supporting both DSTU2 and STU3 versions, though Content Creators omitting the element are restricted to working with FHIR versions STU3 3.0.0 and up.

6.6.6 PhdPatient Resource

Patient information is a highly sensitive issue. To support protection of Personal Health Information (PHI) the RPM Profile supports an option where the Content Creator is given the *logical* id (not the identifier) of a Patient resource by the Content Consumer. How this logical id is obtained is not specified by the RPM Profile. In that case, the Content Creator uses the logical id in all resources that require a reference to a Patient resource. The Content Consumer shall not reject such a resource due to the Patient resource reference, but it does not mean that the reference Patient resource is accessible from the Content Consumer.

If the logical id is not provided by the Content Consumer, the Content Creator is responsible for generating the resource and uploading the resource in such a manner that duplicate resources are not created. The only element required by the PHD patient FHIR profile is the identifier such as the XDSb patient and enterprise identifiers. The Content Consumer provides these values to the Content Creator. How these values are obtained is not specified by the RPM Profile. Since no additional information is required in the case where Patient resource is generated by the Content Creator, this option also allows protection of PHI as long as the enterprise's dictionary mapping patient identifiers to patients is secured.

6.6.7 PhdDevice Resource

The choice of device related resources to represent the PHD properties is for consistency with Point of Care Devices (PoCD) such that the PHD FHIR profile is a subset of the more general PoCD Profile. It could be argued that a more efficient mapping could be created using the Device resource alone and extensions, but this approach would not work for PoCDs.

PHDs expose their specializations, an IEEE EUI-64 system identifier, manufacturer name, model number, production specification (such as serial number and firmware version) information, as well as properties about its real-time clock if the PHD has a real-time clock. PCHA compliant PHDs also expose regulation and certification data.

The PhdDevice resource handles the master specialization, system identifier, and manufacturer name and model number. No other elements are required in the PhdDevice FHIR profile.

6.6.8 PhdDeviceComponent Resource

There will always be at least one PhdDeviceComponent resource associated with the PhdDevice resource. This PhdDeviceComponent contains the production specification information. If the PHD supports multiple specializations, an additional PhdDeviceComponent resource is used to represent the additional specialization analogous to a Virtual Medical Device (VMD) in the 11073-10201 specification upon which PoCDs are based. The additional PhdDeviceComponent references the 'master' PhdDeviceComponent and does not duplicate the production specification information. However, FHIR requirements in DSTU2 and STU3 will mean that certain information is duplicated between the PhdDeviceComponents and the PhgDevice.

6.6.9 PhdDeviceMetric Resource

The PhdDeviceMetric resource contains no information but is only present due to shortcomings in the DSTU2 and STU3 versions of the FHIR specification. Observation resources can only reference Device and DeviceMetrics. It is not possible to reference the DeviceComponent. To avoid orphaning the DeviceComponent, all Phd-related Observation resources reference a PhdDeviceMetric which references a PhdDeviceComponent which references either an additional PhdDeviceComponent or a PhdDevice.

6.6.10 PhgDevice Resource

This resource is used to map the PHG properties. PHGs also have an IEEE EUI-64 system identifier, manufacturer name, model number, production specification, real-time clock properties, regulation, and certification information.

The PhgDevice resource handles the system identifier, and manufacturer name and model number. No other elements are required in the PhgDevice FHIR profile.

6.6.11 PhgDeviceComponent Resource

The PhgDeviceComponent contains the production specification information. However, FHIR requirements in DSTU2 and STU3 will mean that certain information is duplicated between the PhgDevice and PhgDeviceComponents.

6.6.12 PhdNumericObservation Resource

This FHIR profile is used when the PHD sends a numeric metric measurement like a body temperature.

6.6.13 PhdCompoundNumericObservation Resource

This FHIR profile is used when the PHD sends a compound numeric metric measurement like an acceleration or blood pressure.

6.6.14 PhdCodedEnumerationObservation Resource

This FHIR profile is used when the PHD sends an enumeration metric measurement that is an IEEE 11073 code such as a glucose meal context.

6.6.15 PhdBitsEnumerationObservation Resource

This FHIR profile is used when the PHD sends an enumeration metric measurement that is an IEEE 11073 BITs field such as a device and sensor status.

6.6.16 PhdStringEnumerationObservation Resource

This FHIR profile is used when the PHD sends an enumeration metric measurement that is a human readable string such as the cardio specialization exercise program name.

6.6.17 PhdRtsaObservation Resource

This FHIR profile is used when the PHD sends a real-time-sample array (waveform) metric measurement such as an ECG trace.

6.6.18 PhdCoincidentTimeStampObservation Resource

This FHIR profile is used for the coincident time stamp. The coincident time stamp is essentially a ‘measure’ of the PHD’s current time at the current time of the PHG. This information, along with the static time information of the PHD and PHG is used to potentially correct and map the PHD measurement time stamps to local time plus UTC offset.

6.7 RPM Extensions

6.7.1 PchaDeviceProperty Extension

The PchaDeviceProperty extension is used to map the regulation, certification, and static time information. The extension is also used to reference the PCHA Personal Health Gateway (PHG) related device resources.

6.7.2 PhgDeviceReference Extension

The PhgDeviceReference extension is used to point to the Device and DeviceComponent resources describing the Personal Health Gateway properties.

6.8 RPM Data Types

6.8.1 PhdQuantity Data Type

The PhdQuantity is used frequently in the various observation and device-related resources. The main feature of this data type is the use of the IEEE 11073-10101 coding system for the Quantity.system and the UCUM code, which is often similar to a familiar human readable string, for the Quantity.unit. The Quantity.code is the IEEE 11073-10101 code for the unit as sent by the PHD.

6.8.2 PhdTypeCodeableConcept Data Type

The PhdTypeCodeableConcept is used in all the observation-related resources. The main feature of this data type is the required use of the IEEE 11073-10101 coding system for the

CodeableConcept.coding.system and CodeableConcept.coding.code and, if the type happens to be a vital sign, an additional CodeableConcept.coding element with the corresponding CodeableConcept.coding.system and CodeableConcept.coding.code values for LOINC. The LOINC requirement for vital signs is a FHIR requirement.

The data type supports additional CodeableConcept.coding elements in alternative coding systems.

6.6.x.D.1 Referenced Standards

All standards which are reference in this document are listed below with their common abbreviation, full title, and link to the standard.

Table 6.6.2.D.3-2: FHIR - Referenced Standards

Abbreviation	Title	URL
FHIR	Fast Healthcare Interoperability Resources	TBD

Appendices

Appendix J – Communicate PCD Data-hData Transaction Example

The following sequence shows the Communicate PCD Data-hData transaction as it would appear on the wire. For completeness it is assumed the Device Observation Consumer implementation supports an oAuth authentication server and the patient has been registered with the authentication server by the healthcare provider. The healthcare provider has entered the username and password as well as the URL to the Device Observation Consumer server on the Sensor Data Consumer / Device Observation Reporter implementation running on an Android based mobile phone and given it to the patient. Once home, the patient turns on the mobile phone and starts the collector implementation. The patient takes a measurement with a PCHA compliant PHD blood pressure cuff and the data is sent to the phone. The PHD device disassociates and disconnects.

The Device Observation Reporter begins the capabilities exchange. This request is sent using TLS but that is not required.

```
GET /root.xml HTTP/1.1
Content-Type: application/xml
User-Agent: Health@Home-mOXP
Host: 192.168.1.3:8443
```

The Device Observation Consumer responds with the root.xml document containing the server capabilities.

```
HTTP/1.1 200 OK
Server: Jetty/1.9
Content-Type: application/xml
Cache-Control: no-store
Pragma: no-cache
<?xml version="1.0" encoding="UTF-8"?>
<Root xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://hl7.org/schemas/hdata/2013/08/hrf">
    <id>urn:uuid:ab443e5e-b6a7-e951-956c-caef491bbc08</id>
    <version>2.0</version>
    <created>2013-07-14T15:07:38.6875000-05:00</created>
    <lastModified>2013-07-16T08:12:02.2832000-05:00</lastModified>

    <!-- This is the capability exchange -->
    <profile>
        <id>CapabilityExchange</id>
        <reference>http://continuaalliance.org/ccdc/2015/CapabilityExchange</reference>
    </profile>

    <!-- This is the capability for hData Observation upload -->
    <profile>
    <!-- Specified value -->
        <id>observation-upload-hData</id>
        <reference>http://www.continuaalliance.org/upload2013/01/H.812.1.pdf</reference>
    </profile>

    <!-- This is the Unsolicited capability for APS-CDC -->
    <profile>
```



```
        <id>APS-CDC-WAN</id>
        <reference>http://www.continuaalliance.org/hData/APS/2013/01/H.810.2.4.pdf</reference>
    </profile>

    <!-- This is the Unsolicited capability for lampreynetworks.com.private -->
    <profile>
        <id>lampreynetworks.com.private</id>
        <reference>http://lampreynetworks.com./hData/APS/2013/01/LNI Private APS.pdf</reference>
    </profile>

    <!-- This is the capability for oAuth authentication service -->
    <profile>
        <!-- Specified value -->
        <id>oAUTH</id>
        <reference>http://www.continuaalliance.org/upload2013/01/H.810.2.1.pdf</reference>
    </profile>

    <section>
        <!-- chosen by the WAN service; empty on AHD -->
        <path>oAUTH Service</path>
        <port>8441</port>
        <profileID>oAUTH</profileID>
        <resourceTypeID>oAUTH-Bearer</resourceTypeID>
    </section>

    <section>
        <path>pcd01</path>
        <port>8441</port>
        <profileID>observation-upload-hData</profileID>
        <resourceTypeID>observation</resourceTypeID>
    </section>

    <section>
        <!-- This is where an AHD may post ITs root.xml file [baseURL/roots] -->
        <path>roots</path>
        <port>8441</port>
        <profileID>CapabilityExchange</profileID>
        <resourceTypeID>root</resourceTypeID>
    </section>

    <!-- The path the AHD would POST to establish an APS is then: baseurl/APS -->
    <section>
        <!-- chosen by the WAN server; where the AHD does a POST of its APB xml -->
        <path>APS</path>
        <port>8442</port>
        <profileID>APS-CDC-WAN</profileID>
        <!-- optional but recommended -->
        <resourcePrefix>true</resourcePrefix>
        <resourceTypeID>APB</resourceTypeID>
    </section>

    <!-- The path the AHD would POST to establish an APS is then: baseurl/APS -->
    <section>
        <!-- chosen by the WAN server; where the AHD does a POST of its APB xml -->
        <path>APS</path>
        <port>8442</port>
        <profileID>lampreynetworks.com.private</profileID>
        <!-- optional but recommended -->
        <resourcePrefix>true</resourcePrefix>
        <resourceTypeID>APB</resourceTypeID>
    </section>

    <resourceType>
        <id>observation</id>
        <!-- location of reference that describes the Observation upload standard -->
        <reference>http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_TF_Vol2.pdf</reference>
        <representation>
```



```
            <mediaType>application/txt</mediaType>
            <!-- Schema for the resource -->
        </representation>
    </resourceType>

    <resourceType>
        <id>root</id>
        <reference>
               http://www.hl7.org/implement/standards/product_brief.cfm?product_id=261
        </reference>
        <representation>
            <mediaType>application/xml</mediaType>
            <validator>
               http://www.projecthdata.org/hdata/schemas/2013/root.xsd
            </validator>
        </representation>
    </resourceType>

    <resourceType>
        <id>APB</id>
        <!-- location of reference that describes the APS standard -->
        <reference>
http://www.continuaalliance.org/hData/APS/2013/01/ITU_APS_Implementation_Guidelines.docx
        </reference>
        <representation>
            <mediaType>application/xml</mediaType>
            <!-- Schema for the APS xml -->
            <validator>
               http://www.continuaalliance.org/hData/APS/2013/01/APBConfigResource.xsd
            </validator>
        </representation>
    </resourceType>

    <resourceType>
        <id>oAUTH-Bearer</id>
        <!-- location of reference that describes the oAuth standard -->
        <reference>http://tools.ietf.org/html/rfc6750</reference>
        <representation>
           <mediaType>application/json</mediaType>
        </representation>
    </resourceType>
</Root>
```

Note that the Device Observation Consumer server indicates support for an oAuth Bearer token authentication service (highlighted in green) and observation upload using hData (highlighted in yellow). There are ids which link the sets of profile, section, and resourceType elements together to describe the capability. Note that the root.xml indicates support for other features that are, for the moment, outside of the scope of interest for the Remote Patient Monitoring Profile. The Device Observation Reporter ignores these items.

This step does not have to be repeated until the next time the application powers up.

Next the Device Observation Reporter obtains the oAuth Bearer token. The capability exchange indicates where to POST the request. Since entering that capability is optional in the capability exchange (even if the server supports an oAuth authentication server) the URL to such a service may need to be provided to the application via a user interface or some other means. The oAuth request is encrypted using TLS.

```
POST /oAUTH_Service HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Health@Home-mOXP
Host: 192.168.1.3:8443
```



```
Connection: Keep-Alive
Accept: application/x-www-form-urlencoded
Content-Length: 87
grant_type=password&username=Sisansarah&password=publicpassword&scope=ObservationUpload
```

The authentication server checks its data base and sees that user *Sisansarah* with password *publicpassword* has been authorized for the *ObservationUpload* capability transaction. The authentication server responds with the token and a refresh token:

```
HTTP/1.1 200 OK
Server: Jetty/1.9
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
"access_token":"2YotnFZFEjr1zCsicMWpAA",
"token_type":"Bearer",
"expires_in":3600,
"refresh_token":"tGzv3JOkF0XG5Qx2TlKWIA",
"scope":"ObservationUpload"
}
```

The token is good for an hour after which time the refresh token will be needed or a new request made. Thus until the token expires, the Device Observation Reporter can upload as many messages as it wants without repeating the oAuth request.

With the token in hand the upload of the PCD-01 message can start. The capability exchange has indicated to the Sensor Data Source where to POST the PCD-01 message resource. This transaction is encrypted using TLS.

```
POST /pcd01 HTTP/1.1
Content-Type: application/txt
User-Agent: Health@Home-mOXP
Content-Encoding: UTF-8
Host: 192.168.1.3:8443
Connection: Keep-Alive
Accept: application/txt
Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
Content-Length: 2818
MSH|^~\&amp;|LNI Example AHD^ECDE3D4E58532D31^EUI-64|||20130301115450.720-0500||ORU^R01^ORU_R01|
     002013030111545720|P|2.6|||NE|AL|||||IHE PCD ORU-
R012006^HL7^2.16.840.1.113883.9.n.m^HL7&#xD;
PID|||28da0026bc42484^^^&1.19.6.24.109.42.1.3&ISO^PI||Piggy^Sisansarah^L.^^^^L&#xD;
OBR|1|JOXP-PCD^LNI Example AHD^ECDE3D4E58532D31^EUI-64|
     JOXP-PCD^LNI Example AHD^ECDE3D4E58532D31^EUI-64|182777000^monitoring of patient^SNOMED-
CT|||
     20130301115452.000-0500|20130301115455.001-0500&#xD;
OBX|1||531981^MDC_MOC_VMS_MDS_AHD^MDC|0|||||||X|||||||ECDE3D4E58532D31^^ECDE3D4E58532D31^EUI-
64&#xD;
OBX|2|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.1|2^auth-body-continua||||||R&#xD;
OBX|3|ST|532352^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|0.0.0.1.1|5.0||||||R&#xD;
OBX|4|NM|532353^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|0.0.0.1.2|4||||||R&#xD;
OBX|5|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|2^auth-body-continua||||||R&#xD;
OBX|6|CWE|532354^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|0.0.0.2.1|1^unregulated(0)||||||R&#xD;
OBX|7|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.3|2^auth-body-continua||||||R&#xD;
OBX|8|CWE|532355^MDC_REG_CERT_DATA_CONTINUA_AHD_CERT_LIST^MDC|0.0.0.3.1|0^observation-upload-
soap||||||R&#xD;
OBX|9|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.4|532234^MDC_TIME_SYNC_NONE^MDC||||||R&#xD;
```



```
OBX|10|NM|8221^MDC_TIME_SYNC_ACCURACY^MDC
|0.0.0.5|120000000|264339^MDC_DIM_MICRO_SEC^MDC|||||R&#xD;
OBX|11||528391^MDC_DEV_SPEC_PROFILE_BP^MDC|1|||||||X|||||||1234567800112233^^1234567800112233^EUI
-64&#xD;
OBX|12|ST|531970^MDC_ID_MODEL_MANUFACTURER^MDC|1.0.0.1|Lamprey Networks||||||R&#xD;
OBX|13|ST|531969^MDC_ID_MODEL_NUMBER^MDC|1.0.0.2|Blood Pressure 1.0.0||||||R&#xD;
OBX|14|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|1.0.0.3|2^auth-body-continua||||||R&#xD;
OBX|15|ST|532352^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|1.0.0.3.1|2.0||||||R&#xD;
OBX|16|NM|532353^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|1.0.0.3.2|24583~8199~16391~7||||||R
&#xD;
OBX|17|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|2^auth-body-continua||||||R&#xD;
OBX|18|CWE|532354^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|1.0.0.4.1|1^unregulated(0)||||||R&#xD
;
OBX|19|CWE|68219^MDC_TIME_CAP_STATE^MDC|1.0.0.5|1^mds-time-capab-real-time-clock(0)||||||R&#xD;
OBX|20|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|1.0.0.6|532224^MDC_TIME_SYNC_NONE^MDC||||||R&#xD;
OBX|21|DTM|67975^MDC_ATTR_TIME_ABS^MDC|1.0.0.7|20130301115423.00||||||R|||20130301115450.733-
0500&#xD;
OBX|22||150020^MDC_PRESS_BLD_NONINV^MDC|1.0.1|||||||X|||20130301115452.733-0500&#xD;
OBX|23|NM|150021^MDC_PRESS_BLD_NONINV_SYS^MDC|1.0.1.1|105|266016^MDC_DIM_MMHG^MDC|||||R&#xD;
OBX|24|NM|150022^MDC_PRESS_BLD_NONINV_DIA^MDC|1.0.1.2|70|266016^MDC_DIM_MMHG^MDC|||||R&#xD;
OBX|25|NM|150023^MDC_PRESS_BLD_NONINV_MEAN^MDC|1.0.1.3|81.7|266016^MDC_DIM_MMHG^MDC|||||R&#xD;
OBX|26|NM|149546^MDC_PULS_RATE_NON_INV^MDC|1.0.0.8|80|264864^MDC_DIM_BEAT_PER_MIN^MDC|||||R|||201
30301115453.733-0500&#xD;
```

To which the Device Observation Consumer responds

```
HTTP/1.1 200 OK
Server: Jetty/1.9
Content-Type: application/txt

Cache-Control: no-store
Pragma: no-cache
MSH|^~\&amp;|LNI^d0bed0bed0beabee^EUI-64||||20130301115441.444-0500||ACK^R01^ACK|
    00120130301115453695|P|2.6|||NE|AL|||||IHE PCD ORU-
R012006^HL7^2.16.840.1.113883.9.n.m^HL7&#xd;
MSA|AA|00120130301115453695&#xd;
ERR|||0^Message_accepted^HL7|I||||PcdToPHMR: XDS Send was successful. Response: null&#xd;
```

The response message indicates that the PCD-01 message was received with no problems. It also indicates that the message was successfully converted to a PHMR document and sent to the configured destination.

Appendix K – Communicate PCD Data -SOAP Transaction Example

The following sequence shows the Communicate PCD Data-SOAP transaction as it would appear on the wire. For completeness it is assumed the Device Observation Consumer implementation supports an SAML token authentication server using WS-Trust Username Password token and the patient has been registered with the authentication server by the healthcare provider. The healthcare provider has entered the username and password as well as the URL to the Device Observation Consumer server on the Sensor Data Consumer / Device Observation Reporter implementation running on an Android based mobile phone and given it to the patient. Both the URL to the STS Token service AND the observation upload service are provided. Once home, the patient turns on the mobile phone and starts the collector implementation. The patient takes a measurement with a PCHA compliant PHD blood pressure cuff and the data is sent to the phone. The PHD device disassociates and disconnects.

In this case it is assumed that the Device Observation Reporter does not support hData and is, therefore, not going to request a root.xml. The Device Observation Consumer may support both hData as well as SOAP and could have capability elements which give the path to the STS token service as well as the observation upload SOAP service saving the user the effort of entering them.

The WS-Trust STS token request is encrypted using TLS.

```
POST /axis2/services/STS_Username HTTP/1.1
Content-Type: application/soap+xml; charset=UTF-8;
action="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.4; Nexus S Build/IMM26)
Host: 192.168.1.3:8443
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 2414

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security soapenv:mustUnderstand="true"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <wsu:Timestamp wsu:Id="Timestamp-3">
        <wsu:Created>2013-03-01T16:54:53.797</wsu:Created>
        <wsu:Expires>2013-03-01T16:59:53.797</wsu:Expires>
      </wsu:Timestamp>

      <wsse:UsernameToken wsu:Id="UsernameToken-ID">
        <wsse:Username>Sisansarah</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-1.0#PasswordText">
           publicpassword
        </wsse:Password>
      </wsse:UsernameToken>

    </wsse:Security>
    <wsa:To soapenv:mustUnderstand="true">
       https://192.168.1.3:8443/axis2/services/STS_Username
    </wsa:To>
    <wsa:ReplyTo soapenv:mustUnderstand="true">
      <wsa:Address>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:MessageID soapenv:mustUnderstand="true">urn:uuid:0_1362156893800</wsa:MessageID>
```



```
    <wsa:Action
soapenv:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue
    </wsa:Action>
  </soapenv:Header>
  <soapenv:Body>
    <wst:RequestSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
      <wst:Lifetime>
        <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2013-03-01T16:59:53.797</wsu:Created>
        <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2013-03-01T17:04:53.797</wsu:Expires>
      </wst:Lifetime>
      <wst:TokenType>
        http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
      </wst:TokenType>
      <wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey</wst:KeyType>
      <wst:KeySize>256</wst:KeySize>
      <wst:Entropy>
        <wst:BinarySecret Type="http://docs.oasis-open.org/ws-sx/ws-trust/200512/Nonce">
          i369jzmWbYlMB8uEAQwXghli9iORbIRM4IQCQFICrwI=
        </wst:BinarySecret>
      </wst:Entropy>
      <wst:ComputedKeyAlgorithm>
         http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
      </wst:ComputedKeyAlgorithm>
      <wst:Claims Dialect="SomeURI">Continua</wst:Claims>
    </wst:RequestSecurityToken>
  </soapenv:Body>
</soapenv:Envelope>
```

The server responds with

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/soap+xml;action="urn:RequestSecurityTokenResponse";charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 01 Mar 2013 16:54:27 GMT

<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
          soapenv:mustUnderstand="true">
      <wsu:Timestamp wsu:Id="TS-13">
        <wsu:Created>2013-03-01T16:54:27.880Z</wsu:Created>
        <wsu:Expires>2013-03-01T16:59:27.880Z</wsu:Expires>
      </wsu:Timestamp>
    </wsse:Security>
    <wsa:Action soapenv:mustUnderstand="true">urn:RequestSecurityTokenResponse</wsa:Action>
    <wsa:RelatesTo soapenv:mustUnderstand="true">urn:uuid:0_1362156893800</wsa:RelatesTo>
  </soapenv:Header>
  <soapenv:Body>
    <wst:RequestSecurityTokenResponseCollection
          xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
      <wst:RequestSecurityTokenResponse>
        <wst:TokenType>
            http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
        </wst:TokenType>
        <wst:KeySize>256</wst:KeySize>
        <wst:RequestedAttachedReference>
          <wsse:SecurityTokenReference
```



```
     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
            <wsse:Reference URI="#urn:uuid:CCD9102DB9CE26695313621568677 99"
              ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0"/>
          </wsse:SecurityTokenReference>
        </wst:RequestedAttachedReference>
        <wst:RequestedUnattachedReference>
          <wsse:SecurityTokenReference
     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
            <wsse:Reference URI="urn:uuid:CCD9102DB9CE26695313621568677 99"
             ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
/>
          </wsse:SecurityTokenReference>
        </wst:RequestedUnattachedReference>
        <wst:Lifetime>
          <wsu:Created
     xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
             2013-03-01T16:54:27.792Z
          </wsu:Created>
          <wsu:Expires
     xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
             2013-03-01T17:37:39.792Z
          </wsu:Expires>
        </wst:Lifetime>
        <wst:RequestedSecurityToken>

<!-- ============================ Requested SAML Token -->
          <saml2:Assertion
              xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
              xmlns:xs="http://www.w3.org/2001/XMLSchema"
              ID="urn:uuid:CCD9102DB9CE26695313621568677 99"
              IssueInstant="2013-03-01T16:54:27.792Z"
              Version="2.0">
            <saml2:Issuer>LNI SAML Token Service</saml2:Issuer>
              <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                  <ds:Reference URI="#urn:uuid:CCD9102DB9CE26695313621568677 99">
                    <ds:Transforms>
                      <ds:Transform
                           Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces
                          xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"/>
                      </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>hL3WFtfHoQamGfaXGbMfGS7Nn0o=</ds:DigestValue>
                  </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
dldKDhBH2YIAT7hQVdAFn1dbgZtQguJKHNOTz0QtfwAAAKb8iwYZMQuv/DwlgC0cIYprGWqp+4qnpX0Jp3OY8PpQESbrTl9/M
umZcmQYEla8Ojey116mBGPiYmpnp1lNQvwwaZBqvOTChXRj0uns13wRteQy7vx99eQeubneIgo=
                </ds:SignatureValue>
                <ds:KeyInfo>
                  <ds:X509Data>
<ds:X509Certificate>MIICvjCCAiegAwIBAgIES1f+AjANBgkqhkiG9w0BAQUFADCBiTEhMB8GCSqGSIb3DQEJARYSbmFuZ
GFuYUBhcGFjaGUub3JnMQswCQYDVQQGEwJMSzEQMA4GA1UECAwHV2VzdGVybjEQMA4GA1UEBwwHQ29sb21ibzEPMA0GA1UECg
wGQXBhY2hlMRAwDgYDVQQLDAdSYW1wYXJ0MRAwDgYDVQQDDAdzZXJ2aWNlMB4XDTEwMDEyMTA3MTA1OFoXDTM1MDExNTA3MTA
1OFowgYkxITAfBgkqhkiG9w0BCQEWEm5hbmRhbmFAYXBhY2hlLm9yZzELMAkGA1UEBhMCTEsxEDAOBgNVBAgMB1dlc3Rlcm4x
EDAOBgNVBAcMB0NvbG9tYm8xDzANBgNVBAoMBkFwYWNoZTEQMA4GA1UECwwHUmFtcGFydDEQMA4GA1UEAwwHc2VydmljZTCBn
```



```
zANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAlAwDwx/FRgDReNc8Xuzo7/gHejimFkseCm+7WaFZp0dGwTnEJWNwWZk4yMw/1F
qWCgGHAbJBT25TAljleKDMUlZJPaU6PkJD8Hn94A1EstBDYA70pH3wt1moDxYbcG2QLxC1WrFM6aqR3NB92zG8T3Q9X4jxGGW
Pkd39IndfdDMCAwEAAaMxMC8wHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAwIEsDANBgkqhkiG
9w0BAQUFAAOBgQBeAOERzydvAUNipBKOVg3FcjGTyMg3lzo7S1DFg7qTM4FZwUf2zw9XMagVLJRsaw+Asj8mqnugTpB4jBJCr
CGZ7YEviXz4PnqQjuuov5rXtFIc1Bp/PQmQt+LiZ2zln+fFxnSoHEzUsqs5zhdy/uIP0srAtBosdHxL9BJHxd7wQw==</ds:X
509Certificate>
                  </ds:X509Data>
                </ds:KeyInfo>
              </ds:Signature>
              <saml2:Subject>
                <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
                  <saml2:SubjectConfirmationData
                      xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance"
                      NotBefore="2013-03-01T16:54:27.792Z"
                      NotOnOrAfter="2013-03-01T17:37:39.792Z"
                      xsi:type="saml2:KeyInfoConfirmationDataType">
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                      <xenc:EncryptedKey
                         xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                         Id="EK-C82A2592DB5193D51C13621568677947">
                        <xenc:EncryptionMethod
                           Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                          <ds:KeyInfo>
                            <wsse:SecurityTokenReference
    xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
                              <wsse:KeyIdentifier
    EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
    ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#ThumbprintSHA1">
                                EPlMdE3oRiNlo8bGg3BLR3uGWT8=
                              </wsse:KeyIdentifier>
                            </wsse:SecurityTokenReference>
                          </ds:KeyInfo>
                          <xenc:CipherData>
                            <xenc:CipherValue>
JkAWwNH+FdRevF6o9zjB+FTmwxe58jYFeHQO684YNeM5zSLvKna47h/v1OowtnDf5htaBo3uEqp8xPf+IDOYjNQLHfsDHZ60E
vVUjrHKXALE5pRcFtqX93iiUE/Ke4zpVvGQjyMxer454Qo/SL98xd6v4jpDc/zKMK4iGPO+YaI=
                            </xenc:CipherValue>
                          </xenc:CipherData>
                        </xenc:EncryptedKey>
                      </ds:KeyInfo>
                    </saml2:SubjectConfirmationData>
                  </saml2:SubjectConfirmation>
                </saml2:Subject>
              <saml2:Conditions NotBefore="2013-03-01T16:54:27.792Z" NotOnOrAfter="2013-03-
01T17:37:39.792Z" />
                <saml2:AttributeStatement>
                  <saml2:Attribute
                    Name="program"
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
                  <saml2:AttributeValue
                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                       xsi:type="xs:string">
                       Continua
                  </saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
                   Name="user"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
                  <saml2:AttributeValue
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:type="xs:string">Sisansarah</saml2:AttributeValue>
                </saml2:Attribute>
              </saml2:AttributeStatement>
            </saml2:Assertion>
```



```
<!-- ============================= End of SAML Token -->
        </wst:RequestedSecurityToken>
        <wst:RequestedProofToken>
          <wst:ComputedKey>
            http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
          </wst:ComputedKey>
        </wst:RequestedProofToken>
        <wst:Entropy>
          <wst:BinarySecret
            Type="http://docs.oasis-open.org/ws-sx/ws-trust/200512/Nonce">
            2dDQACinnpN2oNV2kFINXEqAN8SMvTQOGpZKB3IAC9c=
          </wst:BinarySecret>
        </wst:Entropy>
      </wst:RequestSecurityTokenResponse>
    </wst:RequestSecurityTokenResponseCollection>
  </soapenv:Body>
</soapenv:Envelope>
```

Note that the username and password in the request is sent in clear text (though encrypted on the wire using TLS). The reason is that the server stores only irreversible hashes of the password which means the server does not know what the password is. If the client sends the password as a hash (which is a WS-Trust Option) the server MUST know the clear-text password in order to validate the request. If a hacker breaks into the server, thousands of passwords could be compromised. On the other hand, if a hacker breaks the client's TLS, only one password is compromised. Examining the "NotBefore" and "NotOnOrAfter" fields in the SAML token indicates that the token is only valid for a little more than 43 minutes. After that time the application will need to request another token before sending more data.

With the SAML token in hand the Device Observation Reporter can upload the PCD-01 document. The message is encrypted using TLS.

```
POST /axis2/services/Exchange HTTP/1.1
Content-Type: application/soap+xml; charset=UTF-8; action="urn:ihe:pcd:2010:CommunicatePCDData"
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.4; Nexus S Build/IMM26)
Host: 192.168.1.3:8443
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 8348

<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security soapenv:mustUnderstand="true"
   xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
   xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
      <wsu:Timestamp wsu:Id="Timestamp-3">
        <wsu:Created>2013-03-01T16:54:54.336</wsu:Created>
        <wsu:Expires>2013-03-01T16:59:54.336</wsu:Expires>
      </wsu:Timestamp>
<!-- ================== SAML Token goes here -->
    </wsse:Security>
    <wsa:To
soapenv:mustUnderstand="true">https://192.168.1.3:8443/axis2/services/Exchange</wsa:To>
    <wsa:ReplyTo soapenv:mustUnderstand="true">
      <wsa:Address>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:MessageID soapenv:mustUnderstand="true">urn:uuid:1_1362156894340</wsa:MessageID>
    <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
  </soapenv:Header>
  <soapenv:Body>
```



```
    <pcd:CommunicatePCDData xmlns:pcd="urn:ihe:pcd:dec:2010">
MSH|^~\&amp;|LNI Example AHD^ECDE3D4E58532D31^EUI-64|||20130301115450.720-0500||ORU^R01^ORU_R01|
     002013030111545720|P|2.6|||NE|AL|||||IHE PCD ORU-
R012006^HL7^2.16.840.1.113883.9.n.m^HL7&#xD;
PID|||28da0026bc42484^^^&amp;1.19.6.24.109.42.1.3&amp;ISO^PI||Piggy^Sisansarah^L.^^^^L&#xD;
OBR|1|JOXP-PCD^LNI Example AHD^ECDE3D4E58532D31^EUI-64|
     JOXP-PCD^LNI Example AHD^ECDE3D4E58532D31^EUI-64|182777000^monitoring of patient^SNOMED-
CT|||
     20130301115452.000-0500|20130301115455.001-0500&#xD;
OBX|1||531981^MDC_MOC_VMS_MDS_AHD^MDC|0|||||||X|||||||ECDE3D4E58532D31^^ECDE3D4E58532D31^EUI-
64&#xD;
OBX|2|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.1|2^auth-body-continua||||||R&#xD;
OBX|3|ST|532352^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|0.0.0.1.1|5.0||||||R&#xD;
OBX|4|NM|532353^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|0.0.0.1.2|4||||||R&#xD;
OBX|5|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|2^auth-body-continua||||||R&#xD;
OBX|6|CWE|532354^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|0.0.0.2.1|1^unregulated(0)||||||R&#xD;
OBX|7|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.3|2^auth-body-continua||||||R&#xD;
OBX|8|CWE|532355^MDC_REG_CERT_DATA_CONTINUA_AHD_CERT_LIST^MDC|0.0.0.3.1|0^observation-upload-
soap||||||R&#xD;
OBX|9|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.4|532234^MDC_TIME_SYNC_NONE^MDC||||||R&#xD;
OBX|10|NM|8221^MDC_TIME_SYNC_ACCURACY^MDC
|0.0.0.5|120000000|264339^MDC_DIM_MICRO_SEC^MDC|||||R&#xD;
OBX|11||528391^MDC_DEV_SPEC_PROFILE_BP^MDC|1|||||||X|||||||1234567800112233^^1234567800112233^EUI
-64&#xD;
OBX|12|ST|531970^MDC_ID_MODEL_MANUFACTURER^MDC|1.0.0.1|Lamprey Networks||||||R&#xD;
OBX|13|ST|531969^MDC_ID_MODEL_NUMBER^MDC|1.0.0.2|Blood Pressure 1.0.0||||||R&#xD;
OBX|14|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|1.0.0.3|2^auth-body-continua||||||R&#xD;
OBX|15|ST|532352^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|1.0.0.3.1|2.0||||||R&#xD;
OBX|16|NM|532353^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|1.0.0.3.2|24583~8199~16391~7||||||R
&#xD;
OBX|17|CWE|68218^MDC_ATTR_REG_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|2^auth-body-continua||||||R&#xD;
OBX|18|CWE|532354^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|1.0.0.4.1|1^unregulated(0)||||||R&#xD
;
OBX|19|CWE|68219^MDC_TIME_CAP_STATE^MDC|1.0.0.5|1^mds-time-capab-real-time-clock(0)||||||R&#xD;
OBX|20|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|1.0.0.6|532224^MDC_TIME_SYNC_NONE^MDC||||||R&#xD;
OBX|21|DTM|67975^MDC_ATTR_TIME_ABS^MDC|1.0.0.7|20130301115423.00||||||R|||20130301115450.733-
0500&#xD;
OBX|22||150020^MDC_PRESS_BLD_NONINV^MDC|1.0.1|||||||X|||20130301115452.733-0500&#xD;
OBX|23|NM|150021^MDC_PRESS_BLD_NONINV_SYS^MDC|1.0.1.1|105|266016^MDC_DIM_MMHG^MDC|||||R&#xD;
OBX|24|NM|150022^MDC_PRESS_BLD_NONINV_DIA^MDC|1.0.1.2|70|266016^MDC_DIM_MMHG^MDC|||||R&#xD;
OBX|25|NM|150023^MDC_PRESS_BLD_NONINV_MEAN^MDC|1.0.1.3|81.7|266016^MDC_DIM_MMHG^MDC|||||R&#xD;
OBX|26|NM|149546^MDC_PULS_RATE_NON_INV^MDC|1.0.0.8|80|264864^MDC_DIM_BEAT_PER_MIN^MDC|||||R|||201
30301115453.733-0500&#xD;
    </pcd:CommunicatePCDData>
  </soapenv:Body>
</soapenv:Envelope>
```

For brevity, the SAML token is not re-printed but its location in the <wsse:Security> header is indicated. The SOAP action “CommunicatePCDData” is present in the WS-addressing action element. Note that both the WS-Trust request and the PCD-01 upload have a time-security element. This element requires that the requests arrive at the server within a five minute window (based on UTC time). A clock skew between the client and server would be enough to cause the request to be rejected even if it were sent in a timely manner.

The Device Observation Consumer then sends the response.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type:
application/soap+xml;action="urn:ihe:pcd:2010:CommunicatePCDDataResponse";charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 01 Mar 2013 16:54:41 GMT

<?xml version='1.0' encoding='UTF-8'?>
```



```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
      soapenv:mustUnderstand="true">
      <wsu:Timestamp wsu:Id="TS-14">
        <wsu:Created>2013-03-01T16:54:41.458Z</wsu:Created>
        <wsu:Expires>2013-03-01T16:59:41.458Z</wsu:Expires>
      </wsu:Timestamp>
    </wsse:Security>
    <wsa:Action
soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDDataResponse</wsa:Action>
    <wsa:RelatesTo soapenv:mustUnderstand="true">urn:uuid:1_1362156894340</wsa:RelatesTo>
  </soapenv:Header>
  <soapenv:Body>
    <pcd:CommunicatePCDDataResponse xmlns:pcd="urn:ihe:pcd:dec:2010">
MSH|^~\&amp;|LNI^d0bed0bed0beabee^EUI-64||||20130301115441.444-0500||ACK^R01^ACK|
    00120130301115453695|P|2.6|||NE|AL|||||IHE PCD ORU-
R012006^HL7^2.16.840.1.113883.9.n.m^HL7&#xd;
MSA|AA|00120130301115453695&#xd;
ERR|||0^Message_accepted^HL7|I||||PcdToPHMR: XDS Send was successful. Response: null&#xd;
    </pcd:CommunicatePCDDataResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

The PCD-01 response message indicates success and the ERR segment indicates that the message was successfully converted to a PHMR and sent to its configured destination.

Volume 3 Namespace Additions

Add the following terms to the IHE Namespace:

NA

