H.812 Services Interface Design Guidelines

Version 2016

August 4, 2016

Table of Contents

Figures

Tables

0 Introduction

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria required to ensure the interoperability of devices and data used for personal connected health. It also contains additional design guidelines for interoperability that further clarify or reduce the options in underlying standards or specifications, or by adding a feature missing in an underlying standard or specification.

These guidelines contain a Services-IF overview, common Design Guidelines for all Services-IF Certified Capability Classes (CCC), and the Design Guidelines for Consent Enabled PHG and Health & Fitness Service CCCs.

Design Guidelines to support the following Certified Capability Classes are defined in separate documents as follows:

- H.812.1 Observation Upload CCC
- H.812.2 Questionnaire CCC
- H.812.3 Capability Exchange CCC
- H.812.4 Authenticated Persistent Session CCC

This guidelines document is one of the “H.810 Interoperability design guidelines for personal health systems” documents [H.810]

0.1 Organization

This document is organized in the following manner.
Clauses 0-5: Introduction and Terminology – These clauses provide Services-IF specific information helpful in comprehending the remainder of this document.
Clause 6: Services-IF Overview - This clause provides an Overview of the Services-IF CCCs.
Clause 7: Use Cases - This clause provides motivating examples.
Clause 8: Behavioral Model - This clause is an overview of sequences of interactions under Services Interface common CCCs and summarizes typical interations, constraints, and exceptions.
Clause 9: Implementation – This clause details the use of common payload content, and SOAP vs REST based transport methodology in the common Services-IF certified capability classes.

0.2 CCC Guideline releases and versioning

Information on releases and versioning of these guidelines can be found in Clause 0.2 [H.810]

0.3 What's New

To see what is new in this release of the design guidelines refer to Clause 0.3 of [H.810]

1 Scope

This guidelines document focuses on the following interface:

- **Services-IF** Interface between Personal Health Gateway (PHG) and Services.

This interface is defined in the Continua architecture as described in [H.810], Clause 5 as shown in Figure 1-1 below.

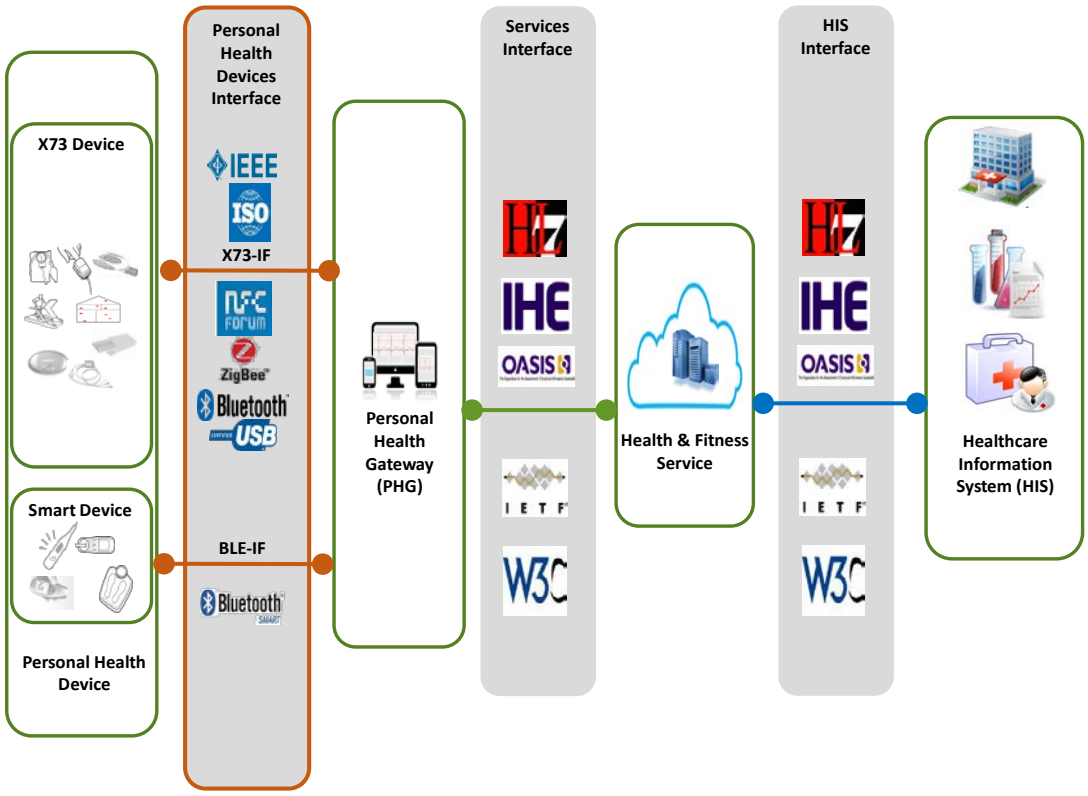

Figure 1-1 – Services Interface in the Continua architecture

There are a number of certified capability classes related to the Services-IF. This document contains interoperability design guidelines that are applicable to several CCCs. Security interoperability design guidelines is one such example. In addition this document also contains the design guidelines for the Consent Enabled PHG and Services Interface CCCs. These CCCs may be grouped with multiple other Services-IF related CCCs, for example, Services Observation Upload or Questionnaire Enabled CCCs.

2 References

All referenced documents can be found in Clause 2 of [H.810]

3 Definitions

This design guideline uses terms defined in [H810]

4 Abbreviations and Acronyms

This design guideline uses abbreviations and acronyms defined in [H810]

5 Conventions

This design guideline follows the Conventions defined in [H810]

6 Architecture

In this End-to-End Reference Architecture, the Services Interface (Services-IF) connects a Personal Health Gateway (PHG) to a Health & Fitness Service. See Figure 6-1 and Figure 6-2 below.
The Services-IF Design Guidelines are focused on enabling the interoperable exchange of information across a Services Interface. A set of Services IF related certified capability classes is defined for the PHG and Health & Fitness Service to enable interoperability for a number of different use cases, including uploading of measurement data, completing questionnaires and executing commands.

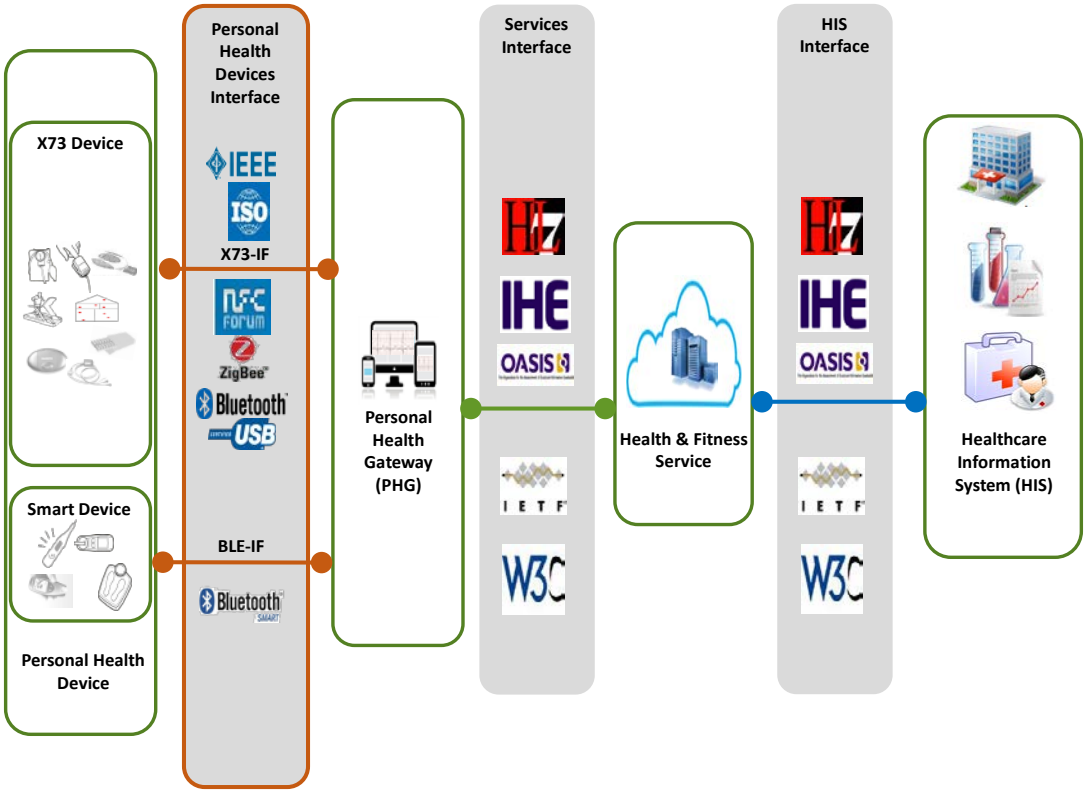

Figure 6-1 – Services Interface

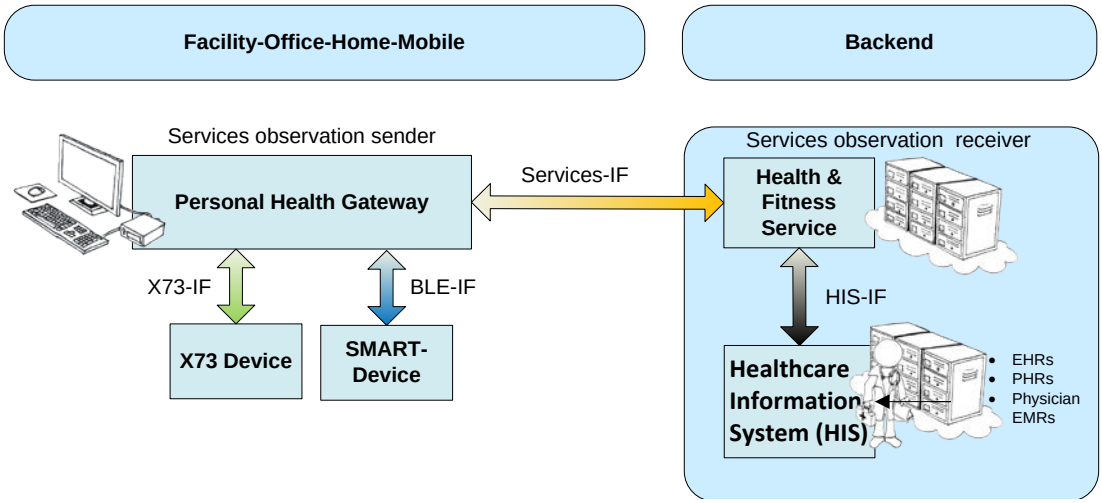

Figure 6-2 – Services-IF examples

In addition to the Services-IF, the End-to-End Reference Architecture also defines the Health Information Services Interface (HIS-IF). The Services-IF is designed to enable granular information exchange between an Personal Health Gateway (typically a PC, laptop, tablet, mobile phone or other type of embedded device), which is a device close to the user/patient and a Health & Fitness Service (typically a backend cloud based service) which collects the information from such users and makes it available for further usage. In contrast the HIS-IF is designed to enable aggregated information exchange between two backend systems, e.g. a disease management system and an electronic health record (EHR)[1]. The HIS-IF is defined in [H.813].

It is also expected that a PHG may be deployed to in-home or user-carried applications, which places a number of constraints on the Services-IF design. Due to the difficulty in maintaining and/or upgrading these devices "in the field", a PHG should be robust/stand-alone and simple enough to keep costs low and technical operational experience/expertise requirements to a minimum. Because of this focus, the Services-IF allows the majority of the contextual metadata associated with the exchange of observations to reside outside of the PHG.

On the other hand, it is expected that a Health & Fitness Service will be a more capable system such as a server or personal computer. Therefore, the design of the Services-IF aims to push complexity and maintainability issues to the Health & Fitness Service if this means that the issues can be avoided on the PHG.

The Services-IF is an abstract channel composed of one or more CCC pairs that connect a PHG Application with a Health & Fitness Service Application. Each CCC pair has a component that resides in the Health & Fitness Service Application and a component that resides in the PHG Application. Continua defines certified capability classes on both sides of the Services-IF.
This version of the Services-IF Guidelines enables the following Certified Capability Classes:

- The uploading of observations from the PHG to the Health & Fitness Service in two different web services styles: (SOAP) and REST (hData) [H.812.1]
- The uploading of consent information from the PHG to the Health & Fitness Service in two different styles: web services (SOAP) and REST (hData) [H.812]
- The downloading of to-be-completed questionnaires from the Health & Fitness Service to the PHG and the uploading of completed questionnaires from the PHG to the Health & Fitness Service [H.812.2]
- The exchange of information (e.g., unsolicited commands) between the Health & Fitness Service and the PHG over an authenticated persistent session [H.812.4]
- The exchange of supported certified capability class information (capability exchange) between the PHG and the Health & Fitness Service as an enabler for the other use cases [H.812.3]

A PHG can support one or more applications that each implements one or more Continua certified capability classes. Figure 6-3 below depicts the Continua Services-IF, showing a PHG Application and a Health & Fitness Service Application in which all of the possible Services-IF certified capability classes are implemented.

[1] *Note: Within the End-to-end architecture both the Services and the Healthcare Information System (HIS) interfaces can be implemented on a device close to the user/patient (PC, laptop, mobile phone, etc) in order to exchange information with entities that are geographically distant from such devices. The Guidelines place no restrictions on the deployment of certified capability classes on specific hardware.*

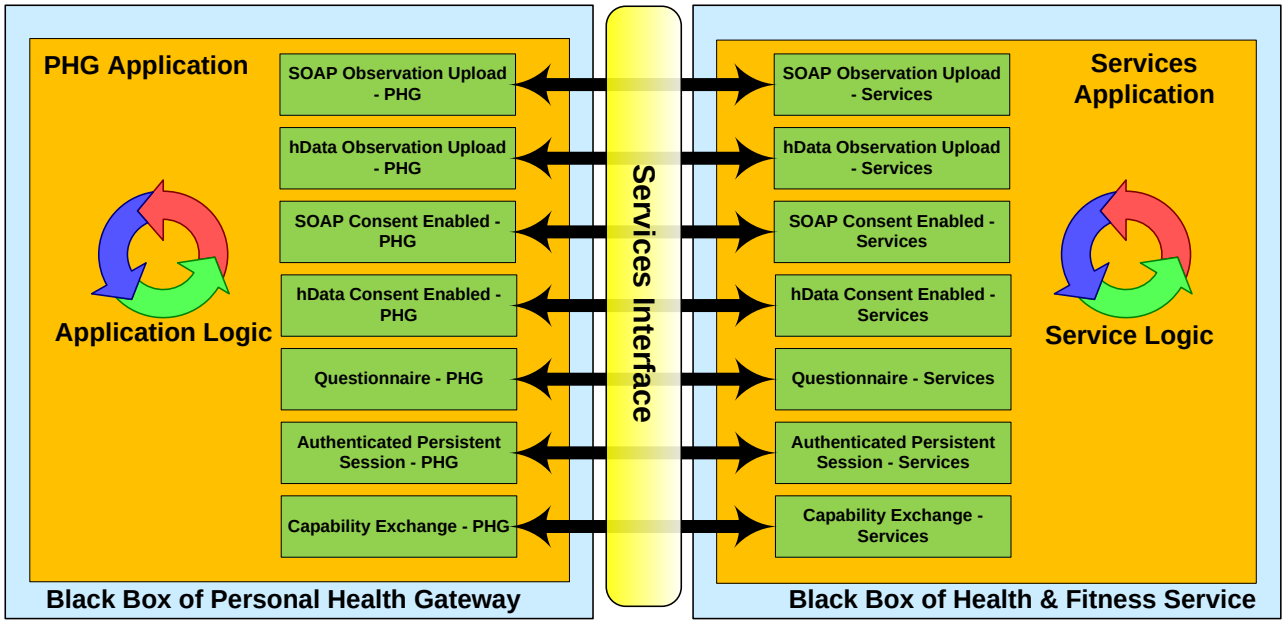

Figure 6-3 – Continua Services-IF showing the Services-IF certified capability classes in this Release

The intent of these Guidelines is to specify system behavior in enough detail to achieve an acceptable level of interoperability for a particular use case. A use case is encapsulated in a Certified Device Class. The Guidelines make normative statements about how the Network Interface of the components of the CCC functions. For the Services-IF these components exist in the context of applications or services that reside on a PHG or a Health & Fitness Service.

Common platforms often limit the manner in which applications can communicate with each other to ensure stability of the overall platform. This limited interaction between applications is called sandboxing. In order to support sandboxed applications this version of the Services-IF uses a reference model that defines an application as a container for one or more CCC components. Interactions between the components within the application container do not have normative requirements and are fully up to the developer of the application. Interactions on the Services-IF between the application's CCCs on the PHG and the corresponding CCCs on the Health & Fitness Service are visible, and do have normative requirements in order to pass certification.

The reference model allows multiple applications to exist in a PHG or Health & Fitness Service, but applications do not interact with other applications except through Network Interfaces. In these Guidelines applications that run on a Health & Fitness Service are often referred to as services since Health & Fitness Services are commonly web service platforms. A Health & Fitness service is conceptually the same as a PHG Application.

These Guidelines document mechanisms by which components may communicate with each other through an internal API. Future versions of the Services-IF may use these mechanisms to enable interoperability between components within an application.

In Figure 6-4 below the concepts of the Services-IF reference model are used to depict a PHG with two independent applications communicating to a Services Application. One PHG Application supports three CCCs and the other supports a single CCC. Normative requirements are made on the Network Interfaces between the PHG and the Health & Fitness Service. The interactions between

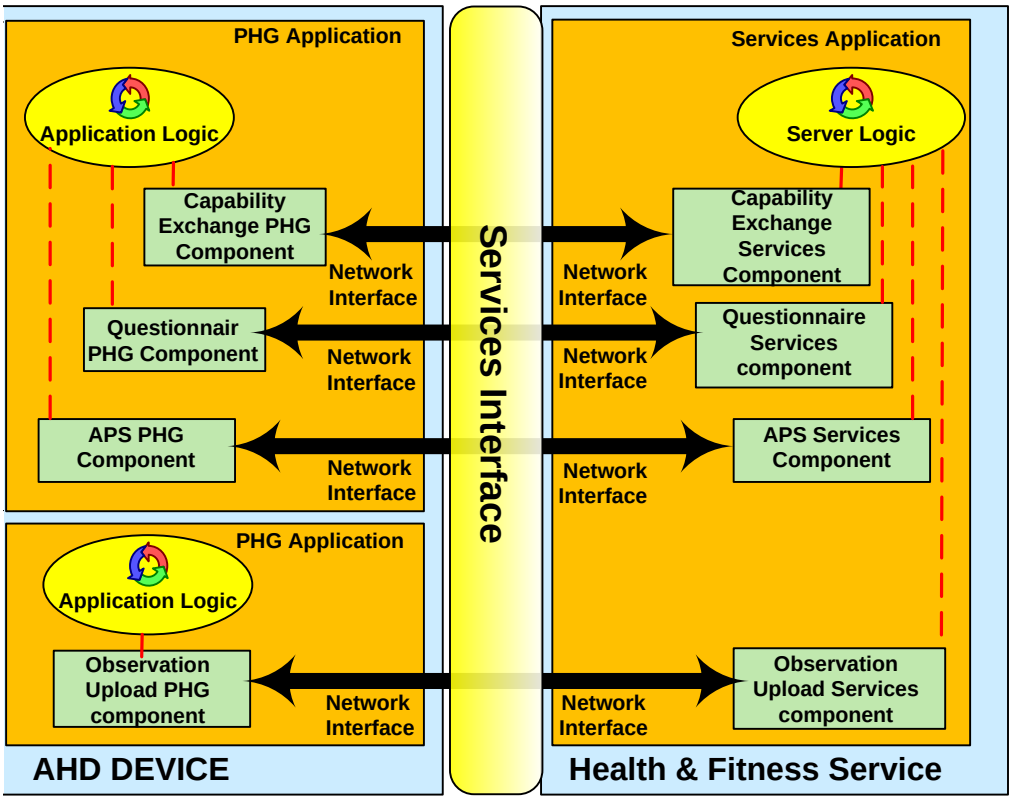

Figure 6-4 – Services-IF Reference Model

the CCC components within an application container are not normative and are shown as red dashed lines coordinated by application internal processing that are out of scope of these Guidelines.

Communications that use the Services-IF start with the PHG's Capability Exchange component. This component sends a request to its peer component on the Health & Fitness Service. The request asks the Health & Fitness service to specify the different certified capability classes it supports. In common language the PHG Application is asking "What things can you do?" The Health & Fitness Service Application answers this in terms of the CCCs it supports. In Figure 6-4 above the Health & Fitness Service Application would say "I support Capability Exchange, Questionnaires, SOAP observation upload and Authenticated Persistent Sessions". When the Capability Exchange component of the Services Application answers the PHG Application, it will typically provide the PHG with additional information, such as a URL, which enables the PHG Application to take the next step in communication with a particular CCC. A PHG that only supports observation uploading using SOAP does not need to implement Capability Exchange. Capability Exchange does not need to be invoked if the PHG is already aware of the capabilities of the Health & Fitness Service.

7 Use Cases

7.1 Consent Management Use Cases

A consent directive is a record of a healthcare client's privacy policy that grants or withholds consent to the Individually Identifiable Health Information (IIHI) [1].

The user consent requirement is derived from different regulations such as HIPAA (Health Information and Portability Accountability Act), EU Directives 95/46, etc. These privacy laws define and assign specific rights to patients with respect to the collection, access, use and disclosure

of their health information. The laws mandate that the patient consent must be obtained before his/her health information may be accessed, used or shared. For example, a patient during registration with a disease management organization (DMO) may be required to fill in a consent form. This consent form captures the patient's acknowledgment and/or signature for a predefined set of policies that specify who is allowed to access his/her IIHI, for what purpose, and how they can use it. This clause introduces the capturing and transferring of consent policy in electronic form on the Continua Services-IF. Digital consent contributes to improved patient empowerment and efficient handling to comply with consent. Examples of patient consent include basic opt-in/opt-out to IIHI, allowing emergency override, limiting access to functional roles (e.g., direct care providers), specific documents to be used for specific research projects, etc.
In a basic scenario a patient will define his consent during or after registering with the Health & Fitness Service Application. How he precisely specifies his consent is out-of-scope for the Continua guidelines, but it could involve selection and possibly adaptation of a default policy using a user interface on his PHG which translates it to a machine readable consent policy representation. Such policies typically contain a reference to the parties involved, data objects and actions that are authorized or not. A Health & Fitness Service Application that receives consent for a particular patient will store it and enforce it for health data that it receives for the patient.
The use cases below are focused on the needs identified for patient consent management.

7.1.1 Upload consent to the server

Adam Everyman registers with an organization e.g. Disease Management Organization (DMO) which remotely monitors patients at home and collects health information from health measurement devices installed at Adam's home. During the time of registration, Adam fills in an eConsent form on the Personal Health Gateway (PHG). The eConsent form consists of options regarding who will be able to access, use, update and disclose different types of vital-signs that are collected through remote patient monitoring system. After specifying preferences, Adam then hits the "submit" button on his telehealth hub. The hub compiles his preferences into a privacy consent directives document which is based on HL7 CDA R2 standard and is then sent from his PHG to DMO which provides remote patient monitoring service. Consent directive then governs access to patient data at the DMO and if Adam's data is sent to third parties (given that this is allowed, e.g., patient's PHR, EHRs, and EMRs), then Adam's privacy consent directive will be associated with the data via the patient identifier.

7.1.2 Retrieve the already completed patient consent from the server

Adam may want to update his privacy preferences e.g. allowing his fitness coach to get access to his data as he has recently registered with a fitness service as suggested by a nurse at the DMO. His PHG provides a link to his latest version of the privacy consent directive document. Adam clicks on the link and PHG then retrieves the latest version of his privacy consent directives from the server and renders it to Adam.

7.1.3 Upload updated consent to the server

Adam reviews his privacy consent preferences and updates them if his fitness coach doesn't have access to his data. After updating consent preferences, he hits the "submit" button on his PHG which then compiles his preferences into a privacy consent directive document that is sent to the DMO. The DMO replaces the old consent with the updated privacy consent directive document.

7.2 Consent Enforcement Use Case

Consent enforcement through encryption protects the privacy of the patient in an efficient manner and makes sure that the content (e.g., observations or response to a questionnaire) is viewed only by

the intended recipient. This prevents viewing of the content by other individuals who may be working in the same organization e.g., administrative staff. The consent enabled Health & Fitness Service should evaluate consent before decrypting the content. Consent is evaluated in order to determine whether the recipient is able to view the content. For example, the process of consent evaluation results in "Success-1" or "Failure-0". The consent enabled Health & Fitness Service should enforce the consent preferences expressed in a consent document.

7.2.1 Content Encryption before upload

Adam Everyman registers with the DMO which remotely monitors him at home and collects health information from health measurement devices installed at his home. Adam Everyman has also registered with a fitness coach as suggested by a nurse at the DMO. Adam Everyman wants his fitness coach to view his activity data and not data from other measurement devices such as blood pressure monitor (BPM). Adam configures his PHG such that now only the nurse at the DMO organization has access to the data from the BPM and activity monitors while the fitness coach only has access to the data from the activity monitors. This is enabled through encryption.

7.3 Other CCC Use Cases

See Clause 6 in design guidelines

- H.812.1 Observation Upload
- H.812.2 Questionnaire
- H.812.3 Capability Exchange
- H.812.4 Authenticated Persistent Session

for their respective CCC Use Cases.

8 Behavioral Models

This clause includes

- Services-IF message exchange behavior
- Security behavior of REST based CCCs
- The Consent Management and Enforcement CCC behavior

8.1 Common Services-IF message exchange Behavior

Due to security and privacy concerns, as well as the technical feasibility of the overall system, the Services-IF requires that all connections be initiated from the PHG. This is illustrated in Figure 8-1. See each design guideline for its message payload and other specifics.

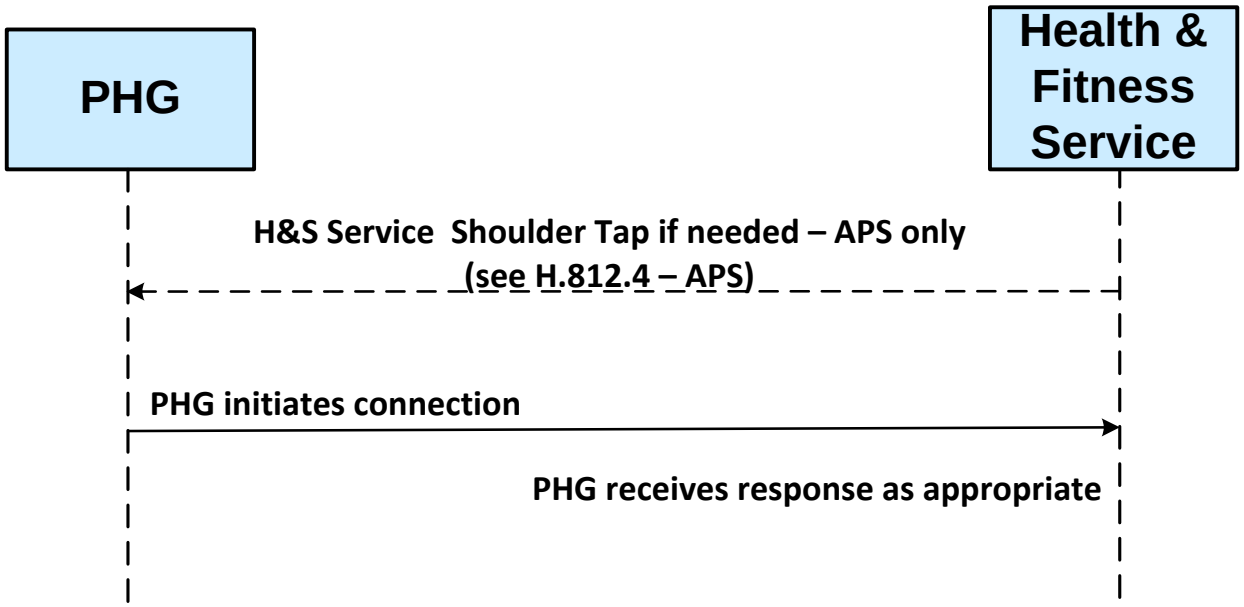

Figure 8-1 – All connections are initiated from PHG

When TLS is required for point to point content security, the use of mutual certificate validation in the TLS handshake is up to the security policy of the Health & Fitness Service.

When authentication is required,

- In the SOAP case, the authentication is a SAML 2.0 token and
- for hData an OAuth 2.0 Bearer token.

How the PHG obtains these tokens is not specified by Continua and it depends upon the trust relationship established between the parties. The Health & Fitness Service Application may support one or more WS-Trust options to obtain SAML 2.0 tokens or it may support an OAuth 2.0 Authorization Framework server using one or more grant types, for example the resource owner password credentials grant type. The Health & Fitness Service may support both services if it supports both hData and SOAP uploads. In either of these cases, an out-of-band operation must take place where the user of the PHG establishes some type of account on the Health & Fitness Service Application allowing the client to obtain these tokens. The Health & Fitness Service token service generates these tokens customized for the recipient which it can validate when it receives the content. On the other hand, the Health & Fitness Service may require that these tokens be obtained from a third party authorization service (such as a CA) which the PHG has established a trust relationship with. In this case, the Health & Fitness Service is letting the third party authorization service validate the client. The Health & Fitness Service may then choose to accept any token that comes from this third party service, or it may additionally choose to pass any received token to the third party authorization service for confirmation before acceptance. The trust relationship details are determined by the security policy of the Health & Fitness Service.

8.2 Common Security model for REST based CCC implementations

Figure 8-2 provides interaction diagram for authorized RESTful transactions based on hData (REST) over HTTP. The authorization is realized using OAuth 2.0 Authorization Framework using resource owner password credentials as authorization grant type. Resource owner password credentials are usually used when there is a high degree of trust between the resource owner (patient) and client (for example, a trusted application running on the application hosting device). In future versions of design guidelines other credential types may be needed based on the use cases where third party

applications (less privileged) may be used to get access to patient's data. The resource owner credentials are used for a single request and are exchanged for an access token. The access token is then used to perform a RESTful transaction on a resource. All interactions with the authorization and resource server are performed in a secure session using [IEEE RFC 4346].

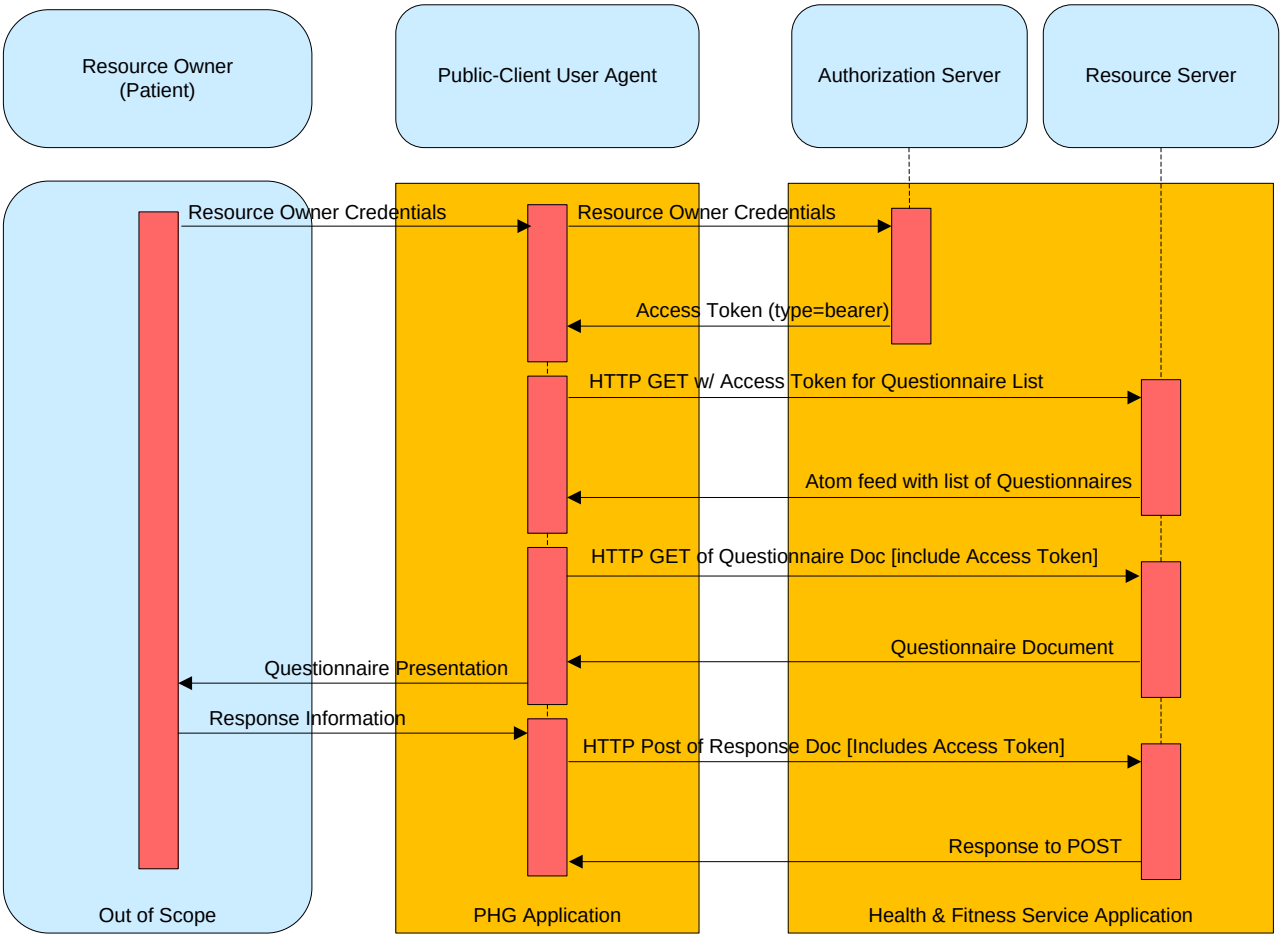

Figure 8-2 – Security Behaviour for authorized RESTful CCC behavior
(Questionnaire use case is taken as an example)

See Table B-1 and Table B-2 for REST CCC Security Guidelines.

8.3 Consent Management Behavioral Model

The following exchange mechanisms are specified for consent management service:

- Create a *new* consent document on the server
- Retrieve *already* specified consent document from the server
- Upload *updated* consent document to the server.

The following diagram illustrates transactions related to the Consent Management use cases described in this content profile.

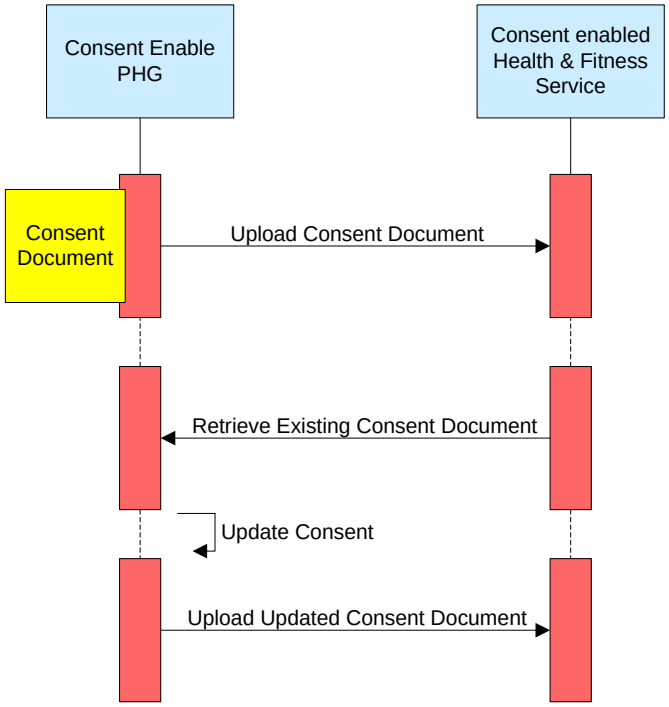

Figure 8-3 – Transactions between PHG and Health & Fitness Service related to consent management

See Table C-1 and Table C-2 for Consent Management Guidelines

8.4 Consent Enforcement Behavioral Model

The following function is specified for the consent enforcement:

- Encrypt to-be uploaded content

The following Figure 8-4 illustrates consent enforcement functionality.

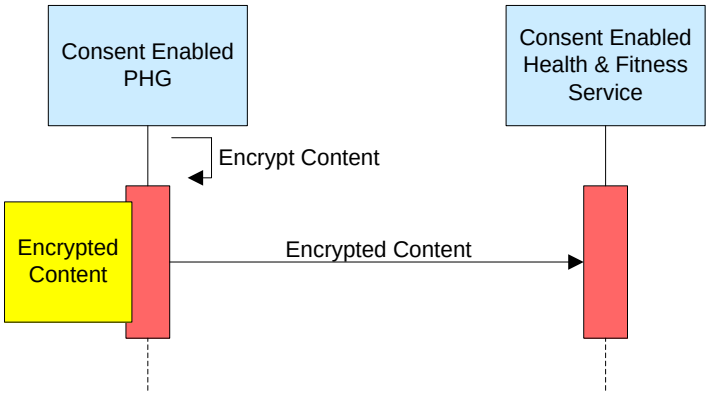

Figure 8-4 – Consent enforcement at the Services-IF

See Table C-3 and Table C-4 for Consent Enforcement Guidelines.

9 Implementation

9.1 Consent Representation

The consent preferences are represented according to the following HL7 standard:

- HL7 Implementation Guide for CDA® Release 2.0: Consent Directive [HL7 CDA CD]

The sample files for a consent document can be found in the submission package for the above mentioned standard.

9.2 Transport Protocols

9.2.1 Transport Protocol using hData over HTTP

In this case, hData over HTTP is used as the transport protocol for the exchange of consent documents across the Services-IF and it supports all use cases that are mentioned in Clauses 7.1 and 7.2. For the detailed requirements on the use of hData over HTTP protocol between PHG and Health & Fitness Services consult Annex A, Table C-1, Table C-2, Table C-3 and Table C-4.

9.2.2 Transport Protocol using IHE XDR

In this case, [IHE ITI TFS XDR] is used as transport protocol for the exchange of consent documents across the Services-IF and supports only Uploading consent to the server use case. Consent documents are linked to the health information (PCD-01 message) via the patient identifier. This way the consent is associated to the health information and thereby controls its use.

9.3 Consent Enforcement

9.3.1 Consent Enforcement using XML Encrypiton

In case of the transport protocol using [IHE ITI TFS XDR], XML encryption standard [W3C XMLENC] is used to enable the consent enforcement through encryption. The XML encryption standard enables encryption of the payload of the PCD-01 transaction for a specific recipient (e.g., doctor or nurse) at the consent enabled Health & Fitness Service.
The XML encryption standard is used to enable consent enforcement through encryption.

9.3.2 Consent Enforcement using IHE DEN

In case of the transport protocol using hData over HTTP, consent enforcement is enabled through the use of the IHE DEN profile [IHE DEN].

Annex A Normative Guidelines Overview

(This annex forms an integral part of this design guideline.)

The Services Certified Capability Classes are listed below:

Table A-1 – Certified Capability Classes

	Certified Capability Classes	Logo-ed Capability Classes
SOAP Observation Upload - PHG	Yes	Yes
SOAP Observation Upload - Health & Fitness Service	Yes	Yes
hData Observation Upload - PHG	Yes	Yes
hData Observation Upload - Health & Fitness Service	Yes	Yes
SOAP Consent Enabled - PHG	Yes	Yes
SOAP Consent Enabled - Health & Fitness Service	Yes	Yes
hData Consent Enabled - PHG	Yes	Yes
hData Consent Enabled - Health & Fitness Service	Yes	Yes
Questionnaire -PHG	Yes	Yes
Questionnaire - Health & Fitness Service	Yes	Yes
Capability Exchange - PHG	Yes	Yes
Capability Exchange - Health & Fitness Service	Yes	Yes
Authenticated Persistent Session - PHG	Yes	*
Authenticated Persistent Session - Health & Fitness Service	Yes	*[2]

[2] * These cells are intentially blank

The guidelines that are applicable for each of the Certified Capability Classes are referenced in Table A-2 below.

Table A-2 – Guidelines for Certified Capability Classes

Certified Capability Classes	Relevant Guidelines
SOAP Observation Upload - PHG	H.812.1, and H.812 Table A-3, Table B-3
SOAP Observation Upload - Health & Fitness Service	H.812.1 , and H.812 Table A-3, Table B-3
hData Observation Upload - PHG	H.812.1 , and H.812 Table A-3, Table B-1
hData Observation Upload - Health & Fitness Service	H.812.1 and H.812 Table A-3, Table B-2
SOAP Consent Enabled - PHG	H.812.1 and H.812 Table A-3, Table B-3 Table C-5, Table C-7
SOAP Consent Enabled - Health & Fitness Service	H.812.1, and H.812 Table A-3, Table B-3, Table C-6, Table C-8
hData Consent Enabled - PHG	H.812 Table A-3, Table C-1,Table C-3 ,Table B-1
hData Consent Enabled - Health & Fitness Service	H.812 Table A-3, Table C-2, Table C-4, Table B-2
Questionnaire - PHG	H.812.2 Table A-1 and H.812 Table A-3, Table B-1
Questionnaire - Health & Fitness Service	H.812.2 Table A-2 and 812 Table A-3, Table B-2
Capability Exchange - PHG	H.812.3 Table A-2 and 812 Table A-3, Table B-1
Capability Exchange - Health & Fitness Service	H.812.3 Table A-1, and 812 Table A-3, Table B-2
Authenticated Persistent Session - PHG	H.812.4 Tables A-1, A-2, A-3, A-5 and H.812 Table A-3, Table B-1
Authenticated Persistent Session - Health & Fitness	H.812.4, Tables A-1, A-4, A-6

Certified Capability Classes	Relevant Guidelines
Service	and H.812 Table A-3, Table B-2

Table A-3 – Requirements common to all CCCs

Name	Description	Comments
CapX-Health & Fitness Service-Universality	All Health & Fitness Services **shall** support Capability Exchange except SOAP based observation upload or consent enabled - Health & Fitness Service CCCs	A Health & Fitness Service that implements only SOAP based observation upload or consent enabled -Health & Fitness Service CCCs is not required to support the Capability Exchange-Health & Fitness Service CCC.
Health & Fitness Service-Transport-Connection-Initiation	All Continua Health & Fitness Service connections **shall** be initiated from the Health & Fitness Service PHG Application and **shall not** be initiated from the Health & Fitness Service	

Annex B General Security Guidelines for Services-IF CCCs

Table B-1 – PHG Security Guidelines using REST

Name	Description	Comments
PHG-Grant-Type	A PHG **may** use Resource Owner Password Credential as Authorization Grant Type as defined in Section 1.3.3 of OAuth v2.0 [IETF RFC 6749].	A PHG may use other means to get authorization token from the authorization server.
PHG-authorization-request	A PHG **may** obtain authorization token from the Authorization Server according to the Section 4.3 and 4.3.2 of OAuth v2.0 [IETF RFC 6749].	See Appendix III for examples of the wire format of the authorization request. See guideline Health & Fitness Service-authorization-request-response for the response
PHG-bearer-token	A PHG **shall** use "bearer" token according to RFC6750 when requesting access to a protected resource on the Health & Fitness Service [IETF RFC 6750].	See the related guideline Health & Fitness Service-authorization-request-response.
PHG-Token-Transmit	A PHG **shall** use the Authorization Request Header Field Method when sending the bearer token as defined in Section 2.1 of RFC6750 [IETF RFC 6749].	
PHG-Confidentiality	A PHG **shall** at minimum use TLS protocol v1.1 for secure point-to-point communication with the authorization server and Health & Fitness Service [IETF RFC 4346].	
PHG-Cipher	A PHG **should** use an encryption cipher suite of TLS_RSA_WITH_AES_128_CBC_SHA	

Table B-2 – Health & Fitness Service Security Guidelines using REST

Name	Description	Comments
Health & Fitness Service-authorization-request-response	A Health & Fitness Service implementing the authorization server **shall** return authorization token of type "bearer" after validating the access token request according to the Section 4.3.3 of the OAuth v2.0 [IETF RFC 6749].	See the guideline PHG-authorization-request for the request format. Authorization could be a separate entity and does not need to be the part of the Health & Fitness Service.
Health & Fitness Service-refresh-token	A Health & Fitness Service implementing the authorization server **shall** return refresh token.	
Health & Fitness Service-Token-Evaluation	A Health & Fitness Service **shall** evaluate the authorization token and its scope before granting access to a record on the Health & Fitness Service.	

Table B-3 – Services IF Transport Security Guidelines

Name	**Description**	**Comments**
Health & Fitness Service-Security-Transport	A Health & Fitness Service Application and PHG Applications **shall** at minimum support the TLS protocol v1.1 [IETF RFC 4346] from WS-I BSP v1.0 for secure communication	This guideline is consistent with the IHE ATNA profile when encryption is enabled. Continua guidelines depend on the guidance in TLS v1.1 (RFC 4346) for mutual authentication

Name	Description	Comments
Health & Fitness Service-Security-Transport-Cipher	A Health & Fitness Service Application and PHG Applications **shall** support AES cipher as specified in [IETF RFC 3268]	IHE ATNA requires the optional use of the following cipher suit: TLS_RSA_WITH_AES_128_CBC_SHA Continua HIS guidelines uses the following cipher suite for security: TLS_RSA_WITH_AES_128_CBC_SHA Other cipher suites are allowed but would need to be negotiated between PHG and Health & Fitness Service
Health & Fitness Service-Confidentiality	A Health & Fitness Service **shall** use TLS protocol v1.1 for secure point-to-point communication with the authorization server and Questionnaire Enabled Health & Fitness Service[IETF RFC 4346].	
Health & Fitness Service-Cipher	A Health & Fitness Service **should** support TLS_RSA_WITH_AES_128_CBC_SHA encryption cipher suite.	

Annex C Normative Guidelines for Consent Management

Table C-1 – Consent Management Guidelines using REST for the Consent Enabled PHG

Name	Description	Comments
PHG-Consent-Enabled	Consent Enabled PHG **shall** comply with HL7 CDA R2 Consent Directive standard for the representation of patient consent preference [HL7 CDA CD].	
PHG-Consent-Enabled-Transport-Standards	Consent Enabled PHG **shall** comply to the following transport standards: HL7 Version 3 Specification: hData Record Format, Release 1 [HL7 hRF] OMG hData REST Binding for RLUS [OMG/hData BIND] OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1 [OMG/hData RLUS]	
PHG-Post-Consent	Consent Enabled PHG **shall** use HTTP POST with the following URL for Posting consent to the Health & Fitness Service: *baseURL/continua/consent*	See the use case in Clause 7.1 For RLUS hData over REST transport, this is performed by performing an HTTP POST request without query parameters at this URL with the privacy consent document in the body of the request.
Consent-Enabled-PHG-Observation-Association	The consent document transmitted by the Consent Enabled PHG **shall** contain the same Patient Identifier as the Health & Fitness Service Observation measurement message(s).	This is to associate the consent document to the Health & Fitness Service Observation measurement messages.
Consent-Enabled-PHG-Observation-Association-Value	The “Patient ID” field in the consent document header **shall** be set to the PID-3 value. Subfields CX-1 and CX-4 **shall** be present and subfield CX-5 **shall** not be present.	

Name	Description	Comments
Consent-Enabled-PHG-Questionnaire Response-Confidentilality	Consent Enabled PHG **shall** set the confidentiality code value to "R" in the header of the Questionnaire Response document.	
Consent-Enabled-PHG-Questionnaire Response-Association-Value	To associate Questionnaire Response documents(s) with a patient consent document, Consent Enabled PHG **shall** use the translation element of the Confidentiality code system as defined in Table IV-3.	See Table IV-1, Table IV-2, and Table IV-4
Retrieving-Consent	Consent Enabled PHG **shall** use HTTP GET with the following URL for retrieving consent from the Health & Fitness Service: *baseURL/continua/consent* Consent Enabled PHG **shall** use HTTP GET with the value of the link element from the ATOM feed entry for retrieving actual consent document from the Health & Fitness Service and **shall** validate that it is a valid HL7 CDA R2 Consent Directive document [HL7 CDA CD].	See the use case in Clause 7.1 For RLUS hData over REST transport, this is performed by performing an HTTP GET request without query parameters at the URL representing patient's consent hData section path which returns the ATOM feed entry. For further info Atom feed entry element consult Table I-1

Table C-2 – Consent Management Guidelines using REST for Consent Enabled Health & Fitness Service

Name	Description	Comments
Consent-Enabled-Health-&-Fitness-Service	Consent Enabled Health & Fitness Service **shall** be able to receive HL7 CDA R2 Consent Directive consent document(s) [HL7 CDA CD].	
Health-&Fitness Service-Consent-Enabled-Transport-Standards	Consent Enabled PHG **shall** comply to the following transport standards: HL7 Version 3 Specification: hData Record Format, Release 1 [HL7 hRF] OMG hData REST Binding for RLUS [OMG/hData BIND] OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1 [OMG/hData RLUS]	

Name	Description	Comments
Health-&-Fitness Service-Consent-Root	Consent Enabled Health & Fitness Service **shall** include the following elements for questionnaire content in the root.xml file: 1. profile a. id=”consent” b. reference=<http://handle.itu.int/11.1002/3000/hData/Consent/2015/01/H.812.pdf> 2. section a. path=”consent” b. profileID= ”consent” c. resourceTypeId=”consent” 3. resourceType a. resourceTypeId=”consent” b. reference=”http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63” c. representation i. mediaType=”application/xml”	Note: The URL given for 1.b reference is an example only
Health-&-Fitness Service-Consent-Validate	Consent Enabled Health & Fitness Service **shall** validate the consent document that it is a valid HL7 CDA R2 Consent Directive document and send the HTTP 200 as a response if it is a valid document.	
Health-&-Fitness Service-Post-Consent-Response	Consent Enabled Health & Fitness Service **shall** create a consent document record after receiving POST message from the Consent Enabled PHG and send the HTTP 201 as a response.	See the PHG-Post-Consent above
PHG-Delete-Consent-Response	Consent Enabled Health & Fitness Service **shall** not support the deletion of an existing consent document record and **shall** return HTTP 405 Method Not Allowed as a response to HTTP DELETE request on a consent URL.	

Table C-3 – Consent Enforcement Guidelines using hData for the Consent Enabled PHG

Name	Description	Comments

Name	Description	Comments
Consent-Enabled-PHG-Content-Encryption-Actor	Consent Enabled PHG **shall** encrypt the content in compliance with IHE Document Encryption (DEN) Profile [IHE DEN].	The content here could be the payload of the PCD-01 transaction or questionnaire response document.
Consent-Enabled-PHG-Questionnaire-Response-MIMEtype	Consent Enabled PHG **shall** set the MIME type to “application/xml” in case the encrypted content is questionnaire response.	The purpose is to indicate the type of the payload that is encrypted.
Consent-Enabled-PHG-Observation - Upload-MIMEtype	Consent Enabled PHG **shall** set the MIME type to “application/txt” in case the encrypted content is observation upload.	The purpose is to indicate the type of the payload that is encrypted.
Consent-Enabled-PHG-Content-Encryption-Algorithm	Consent Enabled PHG **shall** use AES-128 CBC for encryption of the content.	The algorithm used is identified through the ContentEncryptionAlgorithmIdentifier in CMS (Cryptographic Message Syntax) which is further profiled by IHE DEN.
Consent-Enabled-PHG-Encryption-Recipient-Binding-PKI	Consent Enabled PHG **shall** use PKI based key management method from IHE DEN Profile [IHE DEN].	PKI based content key management method uses KeyTransRecipientInfo as CMS RecipientInfoType. This point to the public key or x.509 v3 certificate of the recipient

Table C-4 – Consent Enforcement Guidelines using hData for Consent Enabled Health & Fitness Service

Name	Description	Comments
Health-&-Fitness-Service-Device-HTTP-Ack	Consent Enabled Health & Fitness Service **shall** send the HTTP 202 as a response after successful reception of the encrypted content.	
Consent-Enabled-Health-&-Fitness-Service-Content-Decryption-Actor-XDR	Consent Enabled Health & Fitness Service **shall** comply with IHE DEN Profile to decrypt the encrypted content [IHE DEN].	

Name	Description	Comments
Consent-Enabled-Health-&-Fitness-Service-Key-Management	Consent Enabled Health & Fitness Service **shall** use PKI based key management method as specified by the IHE DEN Profile [IHE DEN].	
Consent-Enabled-Health-&-Fitness-Service-Decryption-Algorithm	Consent Enabled Health & Fitness Service **shall** use AES-128 CBC decryption algorithm for the decryption of the payload.	The algorithm used is identified through the ContentEncryptionAlgorithmIdentifier in CMS (Cryptographic Message Syntax)
Consent-Enabled-Health-&-Fitness-Service-Consent-Enforcement	Consent Enabled Health & Fitness Service **shall** enforce consent preferences expressed in consent document.	E.g., prevents further disclosure of the content to the unauthorized entities

Table C-5 – Consent Management Guidelines using SOAP for the Consent Enabled PHG

Name	Description	Comments
Services-Observation-PHG-Consent	Consent Enabled Services Observation PHG **shall** comply with [HL7 CDA CD] Consent Directive to represent patient consent in a consent document	
Services-Observation-PHG-Consent-Transport	Consent Enabled Services Observation PHG **shall** implement the Document Source actor of IHE XDR to send a consent document using the ITI 41 Provide and Register Document Set-b transaction	

Name	Description	Comments
Services-Observation-PHG-Consent-Frequency	Consent Enabled Services Observation PHG **shall** send the consent document at least once to the Observation Health & Fitness Service	The consent document is e.g., first sent during registration with the service. It is recommended to send consent at least once during the lifetime of connection to observation Health & Fitness Service. Also supports the use cases such as updating consent preferences. The updated consent document is a replacement of the existing consent document at the Consent Enabled Observation Health & Fitness Service
Health-&-Fitness-Services-Observation-Measurement-Consent-Document-Association	The consent document transmitted by the Consent Enabled Services Observation PHG **shall** contain the same Patient Identifier as the Services Observation measurement message(s)	This is to associate the consent document to the Health-&-Fitness-Services Observation measurement messages
Health-&-Fitness-Services-Observation-Measurement-Consent-Document-Association-Value	The "Patient ID" field in the consent document header **shall** be set to the PID-3 value. Subfields CX-1 and CX-4 **shall** be present and subfield CX-5 **shall not** be present	

Table C-6 – Consent Management Guidelines using SOAP for Consent Enabled Health & Fitness Service

Name	**Description**	**Comments**
Observation-Health-&-Fitness-Service-Consent	Consent Enabled Observation Health & Fitness Service **shall** be able to receive, [HL7 CDA CD] Consent Directive consent document(s)	

Name	Description	Comments
Observation-Health-&-Fitness-Service-Consent-Transport	Consent Enabled Observation Health & Fitness Service **shall** implement the Document Recipient actor of IHE XDR to receive a consent document using the ITI 41 Provide and Register Document Set-b transaction	The Observation Health & Fitness Service replaces the existing consent document if a new version was received as indicated by XDS metadata of the consent document

Table C-7 – Consent Enforcement Guidelines using SOAP for the Consent Enabled PHG

Name	Description	Comments
Health-&-Fitness-Services-PHG-Content-Encryption-Actor	Consent Enabled Health & Fitness Services Observation PHG **shall** encrypt the payload (6.5.3 Data Guidelines) of the PCD-01 transaction in compliance with the encryption processing rules defined in the Clause 4.1 of the XML Encryption Specification [W3C XMLENC]	
Health-&-Fitness-Services-PHG-Content-Encryption-MIMEtype	Consent Enabled Health & Fitness Services Observation PHG **shall** set the MIME type to "application/hl7-v2+xml"	The purpose is to indicate the type of payload that is encrypted
Health-&-Fitness-Services-Services-PHG-Content-Encryption-Algorithm	Consent Enabled Health & Fitness Services Observation PHG **shall** use AES-128 CBC as the payload encryption algorithm from the XML Encryption Specification.	The AES-128 CBC algorithm is identified through the use of the following identifier: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]

Name	Description	Comments
Health-&-Fitness-Services-PHG-Encryption-Recipient-Binding-PKI	For the content key transport, Consent Enabled Health & Fitness Services Observation PHG **shall** support RSA Version 1.5 from the XML Encryption Specification	The key transport based on RSA v1.5 is identified through the use of the following identifier [W3C XMLENC]: http://www.w3.org/2001/04/xmlenc#rsa-1_5. For detailed information about RSA v1.5, consult [b-RFC 2437] RSA v1.5 based key transport is also used in CMS (cryptographic message syntax) standard used on the HIS-IF. To find out more, consult [b-RFC 3370] and the consent enforcement guidelines for the HIS-IF
Health-&-Fitness-Services-PHG-Encryption-Recipient-Binding-Symmetric	For the content key transport, Consent Enabled Health & Fitness Services Observation PHG **should** use AES-128 symmetric key wrap algorithm from the XML Encryption Specification. In case of password based encryption, the Consent Enabled Health & Fitness Services Observation PHG **may** use PBKDF2 as the key derivation algorithm from [IETF RFC 3211]	The identifier used for AES-128 symmetric key wrap is "http://www.w3.org/2001/04/xmlenc#kw-aes128" [W3C XMLENC]. The key used in wrapping is referred as KEK, which may be derived from a password or a long term shared secret key
Health-&-Fitness-Services-PHG-Integrity-Payload-PCD-01-Create	Consent Enabled Health & Fitness Services Observation PHG **shall** compute the digest of the encrypted payload using SHA256 (Clause 5.7.2) algorithm according to the XML Encryption Specification	The SHA256 algorithm is identified through the use of the following URL: http://www.w3.org/2001/04/xmlenc#sha256 [W3C XMLENC].

Name	Description	Comments
Health-&-Fitness-Services-Encrypted-Payload-PCD-01-transaction	Consent Enabled Health & Fitness Services Observation PHG **shall** wrap the encrypted payload inside the element <CommunicateEncPCDData xmlns= "urn:ihe:continua:enc:pcd:dec:2012">	In case of the un-encrypted payload the content is wrapped inside the element < CommunicatePCDData xmlns=" urn:ihe:pcd:dec:2010">. See the example in Figure II-1.
Health-&-Fitness-Services-Encrypted-Payload-PCD-01-Transaction-Header	In case of the encrypted payload, the SOAP header **shall** contain "urn:ihe:continua:enc:pcd:dec:2012:CommunicateEncPCDData" instead of "urn:ihe: pcd:dec:2010: CommunicatePCDData"	The plain PCD-01 transaction contains "urn:ihe: pcd:dec:2010:CommunicatePCDData". See the example in Figure II-1, Figure II-2, and Figure II-3

Table C-8 – Consent Enforcement Guidelines using SOAP for Consent Enabled Health & Fitness Service

Name	Description	Comments
Health-&-Fitness-Service-HTTP-Ack	Consent Enabled Observation Health & Fitness Service **shall** send the SOAP HTTP response with the status code equal to 202 after the successful reception of the encrypted message. Consent Enabled Observation Health & Fitness Service **should not** send the PCD-01 application level acknowledgement	The reason is that the observation Health & Fitness Service may not be in possession of the decryption key as the content may be encrypted for a specific recipient on the Health & Fitness Service
Health-&-Fitness-Service-Payload-PCD-01-Verify-Integrity	Consent Enabled Observation Health & Fitness Service **shall** verify the message digest of the encrypted payload	
Health-&-Fitness-Service-Payload-PCD-01-Verify-Integrity-Algorithm	Consent Enabled Observation Health & Fitness Service **shall** support the SHA256 algorithm	

Name	Description	Comments
Health-&-Fitness-Service-Content-Decryption-Actor	Consent Enabled Observation Health & Fitness Service **shall** comply with decryption rules specified in the Clause 4.2 of the XML Encryption Specification [W3C XMLENC].	
Health-&-Fitness-Service-Key-Transport-RSA	Consent Enabled Observation Health & Fitness Service **shall** support RSA Version 1.5 from the XML Encryption Specification [W3C XMLENC].	
Health-&-Fitness-Service-Key-Transport-Symmetric	Consent Enabled Observation Health & Fitness Service **shall** support AES-128 symmetric key wrap algorithm from the XML Encryption Specification [W3C XMLENC]. The Consent Enabled Observation Health & Fitness Service **shall** support PBKDF2 as the key derivation algorithm from [IETF RFC 3211]	The identifier used for AES-128 symmetric key wrap is "http://www.w3.org/2001/04/xmlenc#kw-aes128" [W3C XMLENC]. The key used in wrapping is referred as KEK, which may be derived from a password or a long term shared secret key.
Health-&-Fitness-Services-Content-Decryption-Algorithm	Consent Enabled Observation Health & Fitness Service **shall** use AES-128 CBC decryption algorithm from the XML Encryption Specification [W3C XMLENC].	The AES-128 CBC algorithm is identified through the use of the following identifier: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC].

Appendix I ATOM feed elements for Consent Management

The following ATOM feed child elements of the entry element have a specific usage for the purpose of consent documents.

Table I-1 – ATOM feed child elements for Consent Management

Element	Usage
Author	Person construct that indicates who provided the information in the consent document. i.e. who filed consent
Title	Title of the patient consent document (e.g. Adam's consent authorization)
link	Reference to Adam's consent directive document which shall be a valid HL7 CDAR2 Consent Directive IG document. The link shall be relative and the privacy consent document shall be in the consent section of the hData record.
Published	The published element shall be set to the date and time at which the privacy consent document was posted to the server.

I.1 Information for consent in the root.xml

```
<profile>
   <id>consent</id>

<reference>http://handle.itu.int/11.1002/3000/hData/Consent/2015/01/H.812.pdf</r
eference>
</profile>
<section>
  <path>consent</path>
  <profileID>consentId</profileID>
  <resourceTypeID>consent</resourceTypeID>
</section>
<resourceType>
  <resourceTypeID>consent</resourceTypeID>
  <reference>
    http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63
  </reference>
  <representation>
     <mediaType>application/xml</mediaType>
  </representation>
</resourceType>
```

Appendix II Examples of Consent Management using SOAP

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelop">
   <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-wss-
security-secext-1.0.xsd"
soapenv:mustUnderstand="true" >
      <wsa:To
soapenv:mustUnderstand="true">
https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Service>/wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicatePCDData xmls="urn:ihe:pcd:dec:2010">
            MSH|^~\&|AT4_PHG^123456789ABCDEF^EUI-
            64|||20120409103145+0000||ORU^R01^ORU_R01|MSGID2848518|P|2.6|||NE|AL|||||IHE PCD ORU-
            R012006^HL7^2.16.840.1.113883.9.n.m^HL7 PID|||789567^^^Imaginary
            Hospital^PI||Doe^John^Joseph^^^^L
            OBR|1|POTest^AT4_PHG^1234567890ABCDEF^EUI-64|POTest^AT4_PHG*1234567890ABCDEF^EUI-
            64|182777000^monitoring of patient^SNOMED-CT|||20100903124015+0000
            OBX|1|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.1|532224^MDC_Time_SYNC_NONE^MDC||||||R
            OBX|2|CWE|68220^MDC_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|1^auth-body-continua(2)||||||R
            OBX|3|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|0.0.0.3|1.5||||||R
            OBX|4||528388^MDC_DEV_SPEC_PROFILE_PULS_OXIM^MDC|1||||||X||||||1234567890ABCDEF^EUI-64
            OBX|5|ST|531696^MDC_ID_MODEL_NUMBER^MDC|PulseOx v1.5||||||R
            OBX|6|ST|531970^MDC_ID_MANUFACTURER^MDC|1.0.0.2|AT4 Wireless||||||R
            OBX|7|DTM|67975|^MDC_ATTR_TIME_ABS^MDC|1.0.0.3|20100903124015+0000||||||R20100903124015+
            0000
            OBX|8|CWE|68218^MDC_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|1^auth-body-continua(2)||||||R
            OBX|9|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|1.0.0.5||||||R
            OBX|10|NA|588801^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|1.0.0.6|16388||||||R
            OBX|11|CWE|588802^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|1.0.0.7|0^unregulated-
            device(0)||||||R
            OBX|12|NM|150456^MDC_DIM_PERCENT^MDC|||||R|||20100903124015+0000
            OBX|13|NM|149520^MDC_PULS_OXIM_RATE^MDC|1.0.0.9|71|264864^MDC_DIM_BEAT_PER_MIN^MDC|||||R
            |||20100903124015+0000
         </soapenv:Body>
      </soapenv:Envelop>
```

Figure II-1 – The PCD-01 transaction with un-encrypted payload

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelop">
   <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-wss-
security-secext-1.0.xsd"
   soapenv:mustUnderstand="true">
<wsa:To
soapenv:mustUnderstand="true"
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationCon
sumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns="urn:ihe:continuacenc:pcd:dec:2012">
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType="applicationhl7-v2+xml">
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+"http://www.w3.org/2000/09/xmld sig#">
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#">
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc #rsa-1_5/>
                  <KeyInfo xmlns=http://www.w3.org/2000/09/xmld sig#>
                     <KeyName>John Smith</KeyName>
                  </KeyInfo>
                  <CipherData>
                     <CipherValue>Encrypted Key…</CipherValue>
                  </CipherData>
               </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Figure II-2 – Encrypted PCD-01 transaction – public key based

In Figure II-2, PCD-01 transaction with Encrypted Payload using XML Encryption Standard. The Content key is Encrypted with the Public Key of the Recipient.

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelop”>
   <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-wss-
security-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationCon
sumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:continuacenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmld sig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc #rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmld sig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Figure II-3 – Encrypted PCD-01 transaction – symmetric key based

Figure II-3 shows PCD-01 Transaction with Encrypted Payload using XML encryption standard. In this example, the Content Key is assumed to be known to both sender and recipient and is read only.

Appendix III OAuth Example

Example 1:

- Request for Access Token

In order to obtain access token, Questionnaire Enabled PHG makes the following HTTP POST request to the authorization server.

```
POST http://localhost:3000/oauth2/token HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

grant_type=password&username=john@example.com&password=test
```

Where

- http://localhost:3000/oauth2/token is the URL for reaching authorization server and must be known to the Questionnaire Enabled PHG.
- Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
- This is a basic HTTP authorization header that is generated by Questionnaire Enabled PHG using its given identifier and secret word by encoding them into Base64 hash string Base64("120094574673767:b54dc82476af2814e620b86776c42c0e") =
- "MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl"
- grant_type indicates the authorization code. In this authorization code is username and password.
- Access Token Response

The authorization server validates access token request and if authorized, it generates access token of type "bearer" and optional refresh token.

```
HTTP/1.1 200 OK
Content-Length: 141
Content-Type: application/json
X-Ua-Compatible: IE=Edge
X-Runtime: 0.273027
Server: WEBrick/1.3.1 (Ruby/1.9.3/2013-02-22)
Date: Wed, 03 Apr 2013 08:54:57 GMT
Connection: Keep-Alive

{"access_token":"f779da766bfd1b9164b0fd6d280d52f1","refresh_token":"789f3daf81a302e0636325114113e4b4
","token_type":"bearer","expires_in":899}
```

Where

- "f779da766bfd1b9164b0fd6d280d52f1"is access token that would be used by PHG when accessing a resource on the server.
- "789f3daf81a302e0636325114113e4b4" is refresh token which can be used to obtain a n ew token.
- The token type in the above example is "bearer".
- The lifetime of the token is 899 seconds.
- Requesting a resource using access token of type "bearer"

Example 2:

In the example below the PHG uses a bearer token in order to request a protected resource e.g. questionnaire.

```
GET http://localhost:3000/hdata/root.xml HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Bearer f779da766bfd1b9164b0fd6d280d52f1
```

Appendix IV Consent Enabled PHG Questionnaire Response Association

Table IV-1 – The elements of the confidentiality code system

Name	Value	Comments
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality"	
displayName	"Restricted"	

Table IV-2 – The elements of the Continua Consent Directive code system

Name	Value	Comments
Code	The value **shall** be the same as specified by [HL7 CDA CD].	
codeSystem	2.16.840.1.113883.3.1817 .1.2.1	
codeSystemName	"Continua Consent Directive"	
displayName	ID of the consent document	

Table IV-3 – The translation of the Confidentiality code system to the Continua Consent Directive code system

Name	Value	Comments
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality"	
displayName	"Restricted"	
translation	code="<ID of the consent document>" codeSystem=2.16.840.1.113883.3.1817.1.2.1 codeSystemName="Continua Consent Directive" displayName=ID of the consent document	"<> " is a place holder for the ID of the consent document. Consult Table III-7 for the elements of the Continua Consent Directive code system. For further information about translation construct, consult: <http://dwidgis02.salud.gob.mx/forohl7/html/infrastructure/datatypes_r2/datatypes_r2.htm#dtdl-introduction>

Table IV-4 – OID Distribution for Continua Health Alliance

OID	Description	Comments
2.16.840.1.113883.3.1817	Organization OID: Continua Health Alliance	

OID	Description	Comments
2.16.840.1.113883.3.1817 .1	Root OID for the Continua E2E Architecture	
2.16.840.1.113883.3.1817 .1.2	Root OID for the E2E Security and Privacy	
2.16.840.1.113883.3.1817 .1.3	Root OID for the PAN-IF	
2.16.840.1.113883.3.1817 .1.4	Root OID for the LAN-IF	
2.16.840.1.113883.3.1817 .1.5	Root OID for the TAN-IF	
2.16.840.1.113883.3.1817 .1.6	Root OID for the Services-IF	
2.16.840.1.113883.3.1817 .1.7	Root OID for the HIS-IF	
2.16.840.1.113883.3.1817 .1.2.1	E2E Security and Privacy: OID for the Continua Consent Directive code system	