International Telecommunication Union

ITU-T Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(17 October 2019)

HSTP-H812-FHIR
Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload for trial implementation

ITU-T

International
Telecommunication
Union

Change Log

This document contains Version 2 of the ITU-T Technical Paper HSTP-H812-FHIR on "*Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload for trial implementation*" proposed for Consent at the ITU-T Study Group 16 meeting held in Geneva, Switzerland, 7-17 October 2019.

This version supersedes Version 1, which was approved at the ITU-T Study Group 16 meeting held in Macau, China, 16-27 October 2017.

Editor:	Daidi Zhong Chongqing University P.R.China	Tel: +86-13696454858 E-mail: daidi.zhong@hotmail.com
	Thomas J Erickson PCHA USA	Tel: +1-303-532-9364 E-mail: terickson@pchalliance.org

Technical Paper HSTP-H812-FHIR

Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload for trial implementation

Summary

The Continua Design Guidelines (CDG) defines a framework of underlying standards and criteria that ensure the interoperability of devices and data used for personal connected health services. It also contains design guidelines (DGs) that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

This specification defines guidelines for uploading measurements from a Personal Health Gateway (PHG) to a Health and Fitness Service (H&FS). The uploaded measurements are represented using a resource model consistent with that of HL7 Fast Healthcare Interoperability Resources (FHIR). Although measurements are uploaded using a different encoding and data model than defined in H.812.1, the information content of the delivered measurement is the same.

This Technical Paper is planned to be issued in the future as Recommendation ITU-T H.812.5 as part of the "ITU-T H.810 interoperability design guidelines for personal connected health systems" subseries that covers the following areas:

– ITU-T H.810 – Interoperability design guidelines for personal connected health systems: System overview

– ITU-T H.811 – Interoperability design guidelines for personal connected health systems: Personal health devices interface design guidelines

– ITU-T H.812 – Interoperability design guidelines for personal connected health systems: Services interface design guidelines

– ITU-T H.812.1 – Interoperability design guidelines for personal connected health systems: Services interface: Observation upload capability

– ITU-T H.812.2 – Interoperability design guidelines for personal connected health systems: Services interface: Questionnaires capability

– ITU-T H.812.3 – Interoperability design guidelines for personal connected health systems: Services interface: Capability exchange capability

– ITU-T H.812.4 – Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability

– ITU-T H.812.5 – Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload (planned)

– ITU-T H.813 – Interoperability design guidelines for personal connected health systems: Healthcare information system interface design guidelines

This Technical Paper is based on anticipated directions within the HL7 FHIR community. As such it is a trial implementation specification and subject to change based both on gained experience and final design decisions within HL7 for its FHIR specification.

Table of Contents

Page

List of Tables

Page

List of Figures

Page

0 Introduction

The Continua Design Guidelines (CDG) defines a framework of underlying standards and criteria that ensure the interoperability of devices and data used for personal connected health. They also contain additional design guidelines that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

This document defines guidelines for uploading measurements from a Personal Health Gateway (PHG) to a Health and Fitness Service (H&FS). The uploaded measurements are represented using a resource model consistent with that of HL7 Fast Healthcare Interoperability Resources (FHIR). Although measurements are uploaded using a different encoding and data model than defined in H.812.1, the information content of the delivered measurement is the same.

This document is part of the "ITU-T H.810 interoperability design guidelines for personal health systems" subseries. See [ITU-T H.810] for more details.

0.1 Organization

This Certified Capability Class (CCC) guideline is organized in the following manner:

Clause 0-5: Introduction and terminology - Provides an overview of how H.812.5 is structured

Clause 6: FHIR use cases – A descriptive scenario that motivates the class of problems that FHIR observation upload is addressing.

Clause 7: FHIR observation upload overview – A technical overview of the observation upload process.

Clause 8: Behavioural model – Details of the observation upload process

0.2 CDG guideline releases and versioning

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

0.3 What's New

The initial release of H.812.5 provided the mappings between 11073 objects and FHIR resources. These mappings have been incorporated into [HL7 FHIR IG]. This release of H.812.5 has removed the sections documenting the mappings and references [HL7 FHIR IG]. Updates have been incorporated to replace the use of the deviceComponent resource with the updated FHIR device resource in FHIR 4.0.

A H.812.5 H&FS is no longer required to support XML as a format for observation uploads.

Technical Paper HSTP-H812-FHIR

Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload for trial implementation

1 Scope

This guidelines document defines four Continua Certified Capability Classes associated with uploading a measurement using the FHIR data model defined by HL7 [HL7-FHIR-MODEL]. Two of the capability classes address uploading a sensor measurement when the H&FS supports a FHIR server. In the context of this document a FHIR server is a H&FS that exposes the FHIR API defined by HL7[HL7-FHIR-API]. The remaining two capability classes document how to upload a sensor measurement to a H&FS that does not support a FHIR server. In this case, the FHIR data model is used, but no assumption is made relative to the FHIR server, for example that it persists data.

The Continua Certified Capability Classes defined in this document are:

– FHIR Observation Server – A H&FS that exposes the HL7 FHIR API, and can receive a sensor measurement from a FHIR Observation Client.

– FHIR Observation Client – A PHG that uses the exposed HL7 FHIR API of the H&FS, in a manner defined herein, to transfer sensor measurements.

– FHIR Observation Reporting Server – A H&FS that requires the complete context of a measurement to be contained in the received application data packet. In FHIR this means that the received message contains a complete bundle. A complete bundle is one in which all resources associated with the measurement are present.

– FHIR Observation Reporting Client– A PHG that bundles all resources associated with a given sensor measurement into a single application data packet.

2 References

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

[H.810]	Recommendation ITU-T H.810 (2019), *Interoperability design guidelines for personal connected health systems: Introduction*. https://www.itu.int/rec/T-REC-H.810

3 Definitions

This document uses terms defined in [H.810]

4 Abbreviations and acronyms

This document uses abbreviations and acronyms defined in [H.810]

5 Conventions

This document follows the conventions defined in [H.810].

6 FHIR use cases

In the Continua Design Guidelines (CDGs), capability classes are created to address use cases that meet specific market needs. The four Fast Healthcare Interoperability Resources (FHIR) capabilities classes defined in this document address uploading measurements from a Personal Health Gateway (PHG) to a Health & Fitness Service (H&FS). In that aspect, the FHIR capability classes defined herein serve the same purpose as the capability classes defined in H.812.1. The FHIR capability classes, however, address the additional market requirement for alignment with the wider industry movement toward the use of JavaScript Object Notation (JSON), the FHIR data model, and REST oriented service APIs.

These Guidelines define four FHIR capability classes to address two different business use cases.

The FHIR Observation Server and the FHIR Observation Client are employed when the H&FS supports a FHIR server. This mode of operation is designed for the common use case (e.g. Patient Health Record, Document Sharing, Decision Support), and if employed properly is expected to be more efficient in terms of the network bandwidth consumed for a given upload.

In some business applications, it is not desirable to store patient health information in a FHIR server, but it is still desirable to use the FHIR data model. In this case, the FHIR Observation Reporting Server and FHIR Observation Reporting Client are used to bundle all aspects of a measurement into a single message. The bundling process defined for these capability classes requires that the PHG, acting as the FHIR Observation Reporting Client, place all the FHIR resources needed for a measurement in a single bundle, no external references are allowed. Since all needed information is contained in the bundle, the H&FS, acting as the FHIR Observation Reporting Server, can forward or translate the sensor message without needing to access patient information in a FHIR server. The FHIR Observation Reporting capability classes allow for business relationships to be formed in which the H&FS is only partially trusted.

6.1 Managing patient identity

When a H&FS supports a FHIR server, the PHG must properly reference the patient resource in any observation resource being uploaded. In the FHIR protocol, this is done by having the PHG provide the Logical ID of the patient resource to the FHIR server. How the PHG obtains the Logical ID of the patient resource may be a challenge for a deploying organization. The scenarios in this clause highlight supported methods by which this Logical ID can be obtained. Other methods may work as well.

NOTE – These scenarios apply only to the FHIR Observation Client and FHIR Observation Server.

6.1.1 Scenario #1

In this scenario illustrated in Figure 6-1, the administrative team responsible for the H&FS provides the Logical ID for the Patient Resource. The Logical ID is communicated to the party responsible for configuring the PHG in the home environment. Once the PHG is configured with the appropriate logical identification of the Patient Resource, a measurement can be uploaded using the configured Logical ID of the Patient Resource. An important aspect of this scenario is that the PHG never needs any personal information, and personal information is never seen on the wire.

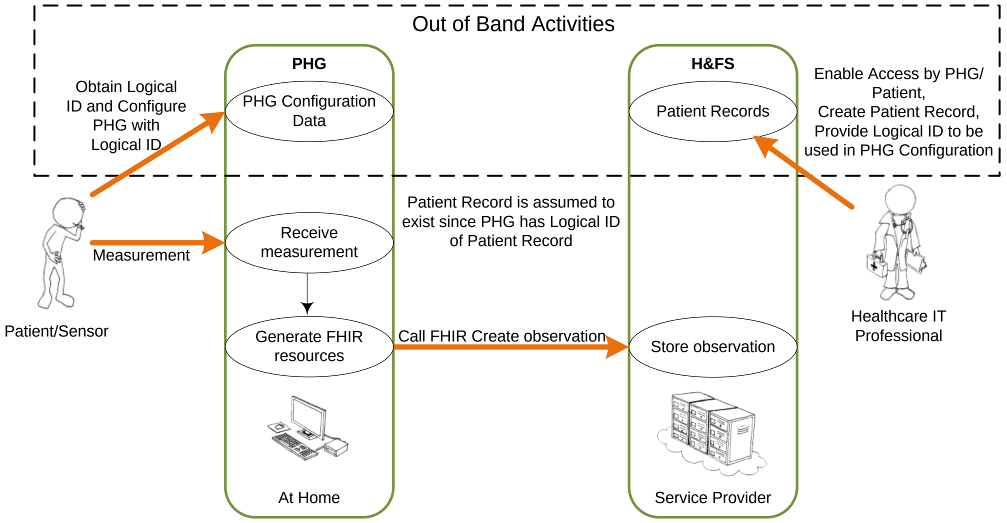
Out of Band Activities
PHG
PHG Configuration Data
H&FS
Patient Records
Obtain Logical ID and Configure PHG with Logical ID
Enable Access by PHG/ Patient,
Create Patient Record,
Provide Logical ID to be used in PHG Configuration
Patient Record is assumed to exist since PHG has Logical ID of Patient Record
Receive measurement
Measurement
Patient/Sensor
Generate FHIR resources
Call FHIR Create observation
Store observation
Healthcare IT Professional
At Home
Service Provider

Figure 6-1 – Scenario #1 FHIR observation upload

6.1.2 Scenario #2

In scenario 2, the administrative team for the H&FS does not provide the patient with the FHIR Logical ID of the Patient Resource. Instead, other information, which identifies the patient and is herein called the Patient Designator, is used to establish the identity of the patient in the uploading of a measurement.

NOTE – An insurance card where the card's issuer (an insurance company) is an assigning authority, and the account number on the card identifies the patient to the insurance company) is an example of a patient designator. The backend FHIR server would be configured with this information in *Patient.identifier.system* and *Patient.identifier.value* within the Patient Resource.

The Patient Designator can represent a wide range of different forms of patient identity, appropriate to different situations. The Patient Designator contains information about who the assigning authority is, and how the patient is identified by that assigning authority. In general, the Patient Designator is a method some organizations may use to identify a patient, and by itself does not expose personal information. In many cases, the Patient Designator may be familiar to the patient through other communications with the organization. As shown in Figure 6-2, the Patient Designator is used to generate a FHIR Patient Resource and the PHG takes the responsibility of specifying the Logical ID of this resource, which must be unique when used in the FHIR server. The PHG uses the generated Logical ID to create a Patient Resource on the FHIR server, or to confirm the pre-existence of the Patient Resource. Once the PHG has obtained and validated the Logical ID of the Patient Resource on the FHIR server, it can upload measurements and reference the Patient Resource via the Logical ID.

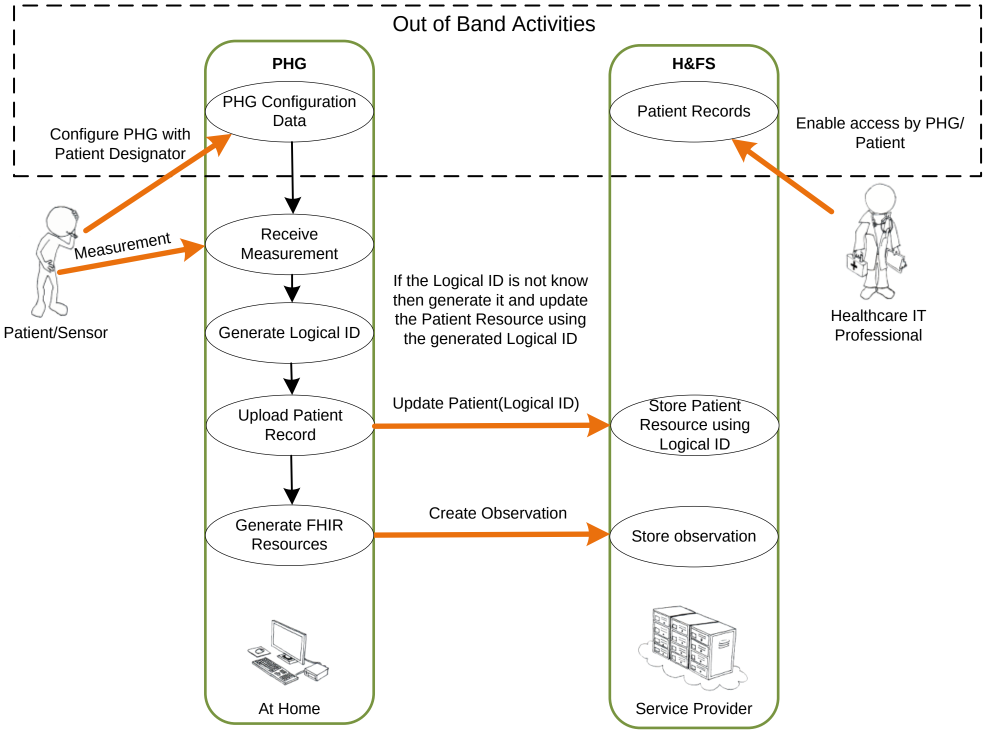
Out of Band Activities
PHG
PHG Configuration Data
Receive Measurement
Generate Logical ID
Upload Patient Record
Generate FHIR Resources
At Home
H&FS
Patient Records
Store Patient Resource using Logical ID
Store observation
Service Provider
Configure PHG with Patient Designator
Measurement
Patient/Sensor
If the Logical ID is not know then generate it and update the Patient Resource using the generated Logical ID
Update Patient(Logical ID)
Create Observation
Enable access by PHG/ Patient
Healthcare IT Professional

Figure 6-2 – Scenario #2 FHIR observation upload

6.1.3 Scenario #3

In the third scenario, the patient is provided with the Patient Designator, but in contrast to scenario 2, the Patient Resource Logical ID is generated by the FHIR server on the H&FS. The PHG obtains the generated Logical ID by identifying the Patient Resource using the Patient Designator. The patient resource must have been previously provisioned on the FHIR server, or the PHG must be allowed to create a new Patient Resource. The patient experience is the same in this scenario as in scenario 2. This scenario is included since an organization running an H&FS may not be comfortable with the idea of the PHG defining the Logical ID for a Patient Resource on the FHIR server for which they are responsible.

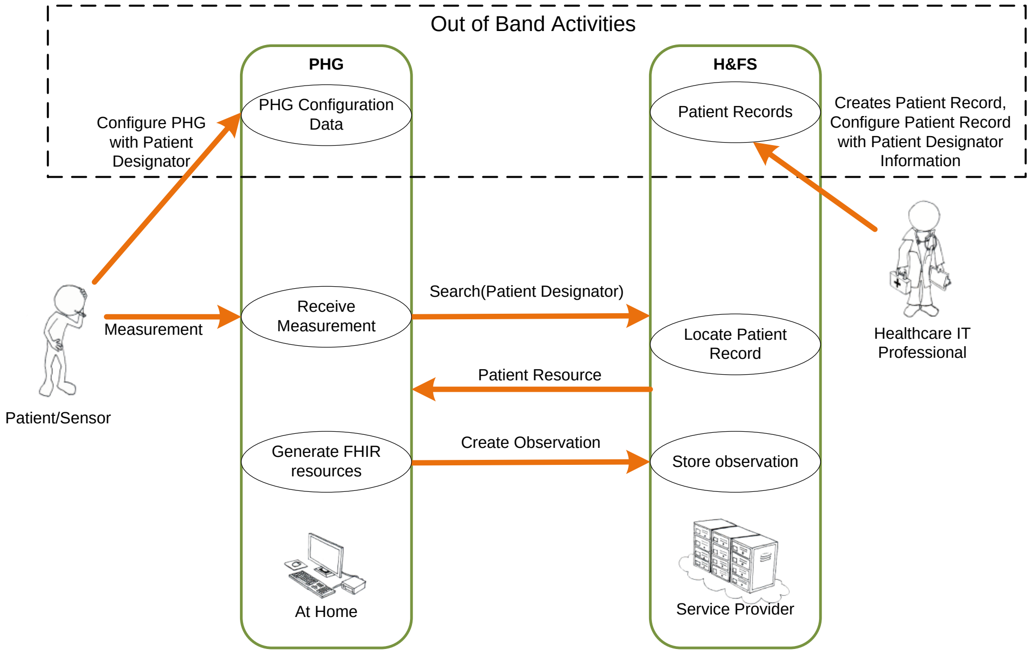

Figure 6-3 – Scenario #3 FHIR observation upload

6.1.4 Scenario #4

In this final scenario, the identification of the patient resource and its associated Logical ID is established using OAuth. Inherent in the use of OAuth is an authentication procedure of some type that defines the access rights granted to the PHG. The authentication procedure establishes a user identity that is granted access to the resources associated with a specific patient record. A FHIR GET operation requesting all patient resources returns nothing or a single patient resource and its associated Logical ID since the PHG is only authorized to see one patient record. The Logical ID is then used to upload the measurement. The primary advantage of this approach is that the patient does not have to be provided with a Patient Designator or a Logical ID.

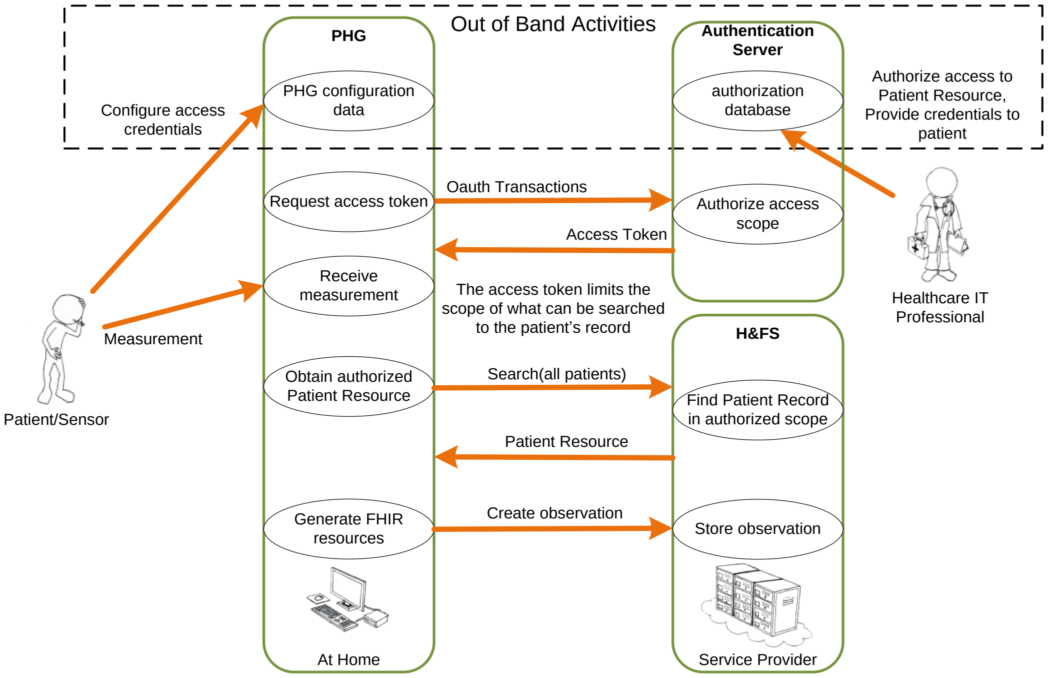

Figure 6-4 – Scenario #4 FHIR observation upload

7 Background (informative)

The HL7 FHIR specifications define a collection of resources that can be used to support a broad spectrum of Healthcare workflows. This CDG document specifies how to use the HL7 FHIR resources to model observations that can be received from a Continua PHD, and how to securely upload the observations to an H&FS. This CDG also identifies how to map the ISO/IEEE 11073 fields and values into the corresponding FHIR resource representation.

The FHIR Certified Capabilities Classes are defined to be part of the Services Interface. As depicted in the Continua Architecture (Figure 7-1**)**, the Services Interface is associated with communication between the PHG and the H&FS.

NOTE – The reader should be aware that the Continua Architecture represents a functional architecture created for defining behaviour between components. It does not define how a given system is to be deployed. For instance, a logical PHG may reside inside a sensor device.

Figure 7-1 depicts FHIR usage within the Continua Architecture.

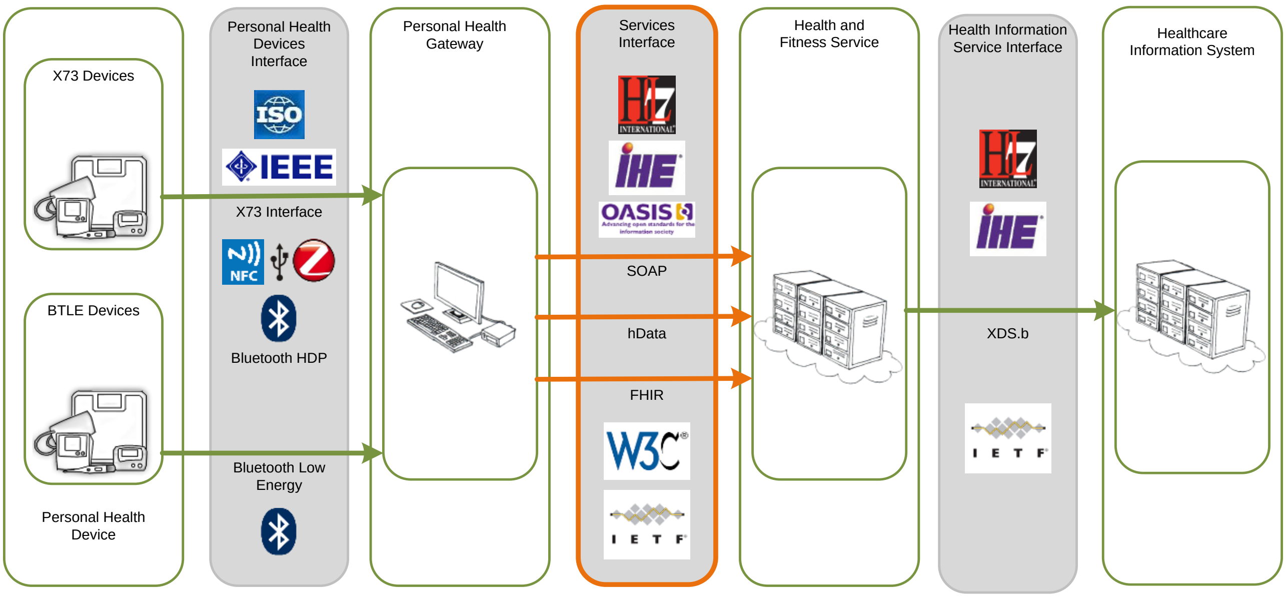

Figure 7-1 – Continua reference architecture

A FHIR observation upload is normally preceded by a PHD delivering an observation to a PHG. The communications between the PHD and the PHG allows two or more ISO/IEEE 11073 objects types to be constructed by the PHG. The first object type is the Medical Device System (MDS) of the PHD, which provides information about the PHD. The second object type is the ISO/IEEE 11073 metric object type which represents the observation (measurement) taken by the PHD. There may be multiple metric objects types from a single measurement process of a PHD.

The PHG maps the ISO/IEEE 11073 objects types from the PHD along with its own MDS [H.812.1] and configured patient information to FHIR resources. The mapping may create instances of three FHIR resource types:

– Patient resource: Demographic and administrative information about the patient.

– Device resource: Characteristics, operational status and capabilities of a healthcare device.

– Observation resource: Measurements or assertions about a subject. Can be a patient or a device.

See the [HL7 FHIR IG] for detailed information on mapping between ISO/IEEE 11073 objects and FHIR resources.

7.1 Security framework

FHIR resources are uploaded to the H&FS in the context of an encrypted TCP connection with authorization to upload being provided through OAuth [OAuth 2.0]. To upload the FHIR resources, the PHG must have an OAuth bearer token. If it does not have a valid bearer token, the PHG communicates with the OAuth Server to obtain one.

Continua certification is designed to ensure interoperability between components marketed by different organizations. To ensure that a minimum level of interoperability is possible when OAuth is used for securing the uploading of measurements with FHIR, a certified PHG is required to support one of: (1) client credential, (2) resource owner, (3) authorization code, or (4) implicit grant types. A certified H&FS is required to support both the client credential and the resource owner credential authorization grants. Further, if the H&FS claims to work with browser based PHGs, then it must also support Authorization Code and Implicit grant types.

NOTE – Continua certification means that the certified product has support for the required grant types and provides a mechanism by which the grant types could be enabled. Continua certification does not mean that a certified product, when deployed, must enable that support.

In addition to the required OAuth grant types, this specification profiles the usage of the *Assertion Framework for OAuth Client Authentication* [OAuth Assertion] in conjunction with *JSON Web Token Profile for OAuth Client Authentication and Authorization Grants* [OAuth JWT] to enable assertion-based authorization of PHGs. The use of JSON web token-based OAuth authorization is optional for both the PHG and the H&FS.

Although OAuth provides a standardized mechanism by which authorization can be granted to a PHG for uploading a message, it does not define how the FHIR resources within the H&FS are secured. The business logic associated with a given H&FS is ultimately responsible for ensuring the security of the information in the H&FS; this CDG document does not specify how FHIR security is achieved by the H&FS.

7.2 Example uploads from a FHIR observation client

The examples in this section illustrate the exchanges that would take place between a PHG and a H&FS for each of the different scenarios listed in clause 6. The examples assume the use of a resource owner access grant in the OAuth exchange, and that the PHG is using Capability Exchange. The Examples in this section also assume that the upload is taking place between a FHIR Observation Client and FHIR Observation Server.

To simplify the sequence diagrams neither the Capability Exchange nor the OAuth exchange sequences are shown in full. For reference, the full steps are listed below.

Capability Exchange:

1. The PHG is configured with the URL base address where it can obtain the root.xml file.
2. The PHG issues a GET to obtain the root.xml file.
3. The PHG builds the URL to the atom feed from the content of the root.xml and issues an http GET to obtain the atom feed for the OAuthDescriptors.
4. The PHG uses the link reference in the entry element of the returned atom feed to obtain the URL of the OAuthDescriptor itself.
5. The PHG issues a GET to obtain the OAuthDescriptor

OAuth Exchange when using a Resource Owner Grant type:

1. The PHG OAuth client application has been pre-configured with a client_id and associated client_secret.
2. The PHG OAuth client application sends an OAuth Authorization request to the resource owner.

   NOTE – This step may be implemented by the PHG OAuth client code looking up configuration information that has been provided by the resource owner, or by the PHG OAuth client code displaying an input window in which the resource owner enters credential information. This document does not require that the PHG implement a visible OAuth exchange to an authorization server's authorization endpoint.
3. The PHG OAuth client code obtains the resource owner credentials
4. The PHG issues a request to the authentication server's token endpoint with the grant type parameter set to indicate the user of a resource owner password. The resource owner's credentials are provided along with the client_id and client_secret, and optionally the scope.
5. The authentication server returns the bearer token and possibly modified scope to the PHG OAuth client code.

In clauses 7.2.1 – 7.2.4, each scenario identified in clause 6 is illustrated with numbered steps and a sequence diagram.

7.2.1 Scenario #1

1. The H&FS is configured with a Patient Resource, generating a FHIR Logical ID.
2. The PHG is loaded with the FHIR Logical ID for the Patient Resource created on the H&FS, the H&FS URLs, the client id, the resource owner id, and the password.
3. The PHG performs Capability Exchange with the H&FS to discover the H&FS FHIR upload capabilities.
4. An observation is taken on the health sensor; the sensor communicates the measurement to the PHG.
5. The PHG receives the measurement and associates the measurement with a patient to obtain the Patient Record Logical ID.
6. The PHG recognizes that it does not have a valid access token or refresh token. The PHG sends a resource owner grant request to the OAuth authorization server's token endpoint which includes the client id, the resource owner credentials, and the scope.
7. The OAuth token endpoint validates the credentials in the context of the scope and sends an authorization grant in the form of a bearer token.
8. The PHG creates the necessary FHIR resources from the received sensor measurement and internal PHG data.
9. The created FHIR resources are uploaded to the FHIR resource server URL obtained from the Capability Exchange Process.
10. The H&FS validates the authorization using the bearer token, and if access is granted stores the FHIR resources in the context identified by the Patient Resource Logical ID.
11. The H&FS server returns the appropriate HTTP response.

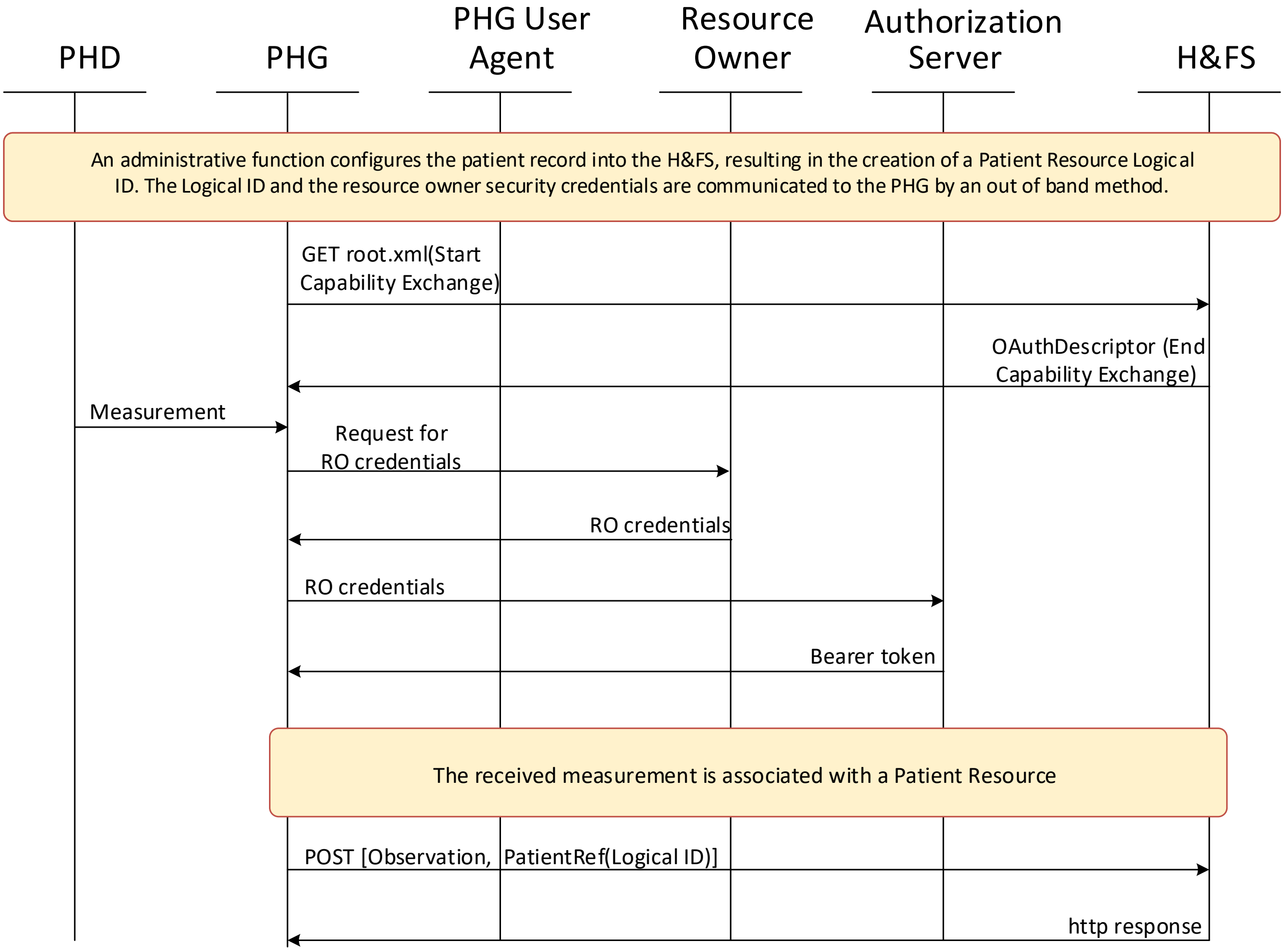
PHD
PHG
PHG User Agent
Resource Owner
Authorization Server
H&FS
An administrative function configures the patient record into the H&FS, resulting in the creation of a Patient Resource Logical ID. The Logical ID and the resource owner security credentials are communicated to the PHG by an out of band method.
GET root.xml(Start Capability Exchange)
OAuthDescriptor (End Capability Exchange)
Measurement
Request for RO credentials
RO credentials
RO credentials
Bearer token
The received measurement is associated with a Patient Resource
POST [Observation, PatientRef(Logical ID)]
http response

Figure 7-2 – Scenario #1 sequence diagram

7.2.2 Scenario #2

1. The PHG is loaded with the Patient Designator, the H&FS URLs, the client id, the resource owner id, and the password.
2. The PHG performs Capability Exchange with the H&FS to discover the H&FS FHIR upload capabilities.
3. The PHG receives a measurement from the sensor.
4. The PHG recognizes that it does not have a Logical ID for the patient associated with the measurement and creates a FHIR Patient Resource, generating a Logical ID in the process.
5. The PHG recognizes that it does not have a valid access token or refresh token. The PHG sends a resource owner grant request to the OAuth authorization server's token endpoint which includes the client id, the resource owner credentials, and the scope.
6. The Authentication Server validates the credentials in the context of the scope and sends an authorization grant in the form of a bearer token.
7. The PHG sends the Patient Resource to the H&FS in conjunction with the access token.
8. The PHG creates the necessary FHIR resources to upload the measurement from the received sensor measurement and internal PHG information.
9. The FHIR resources are uploaded to the URL obtained from the Capability Exchange Process using the Logical ID of the Patient Resource to provide patient context.

10. The H&FS validates the authorization using the bearer token, and if access is granted stores the FHIR Observation Resource, and, if provided, the Device resource in the context identified by the Patient Resource Logical ID.

11. The H&FS server returns the appropriate HTTP response.

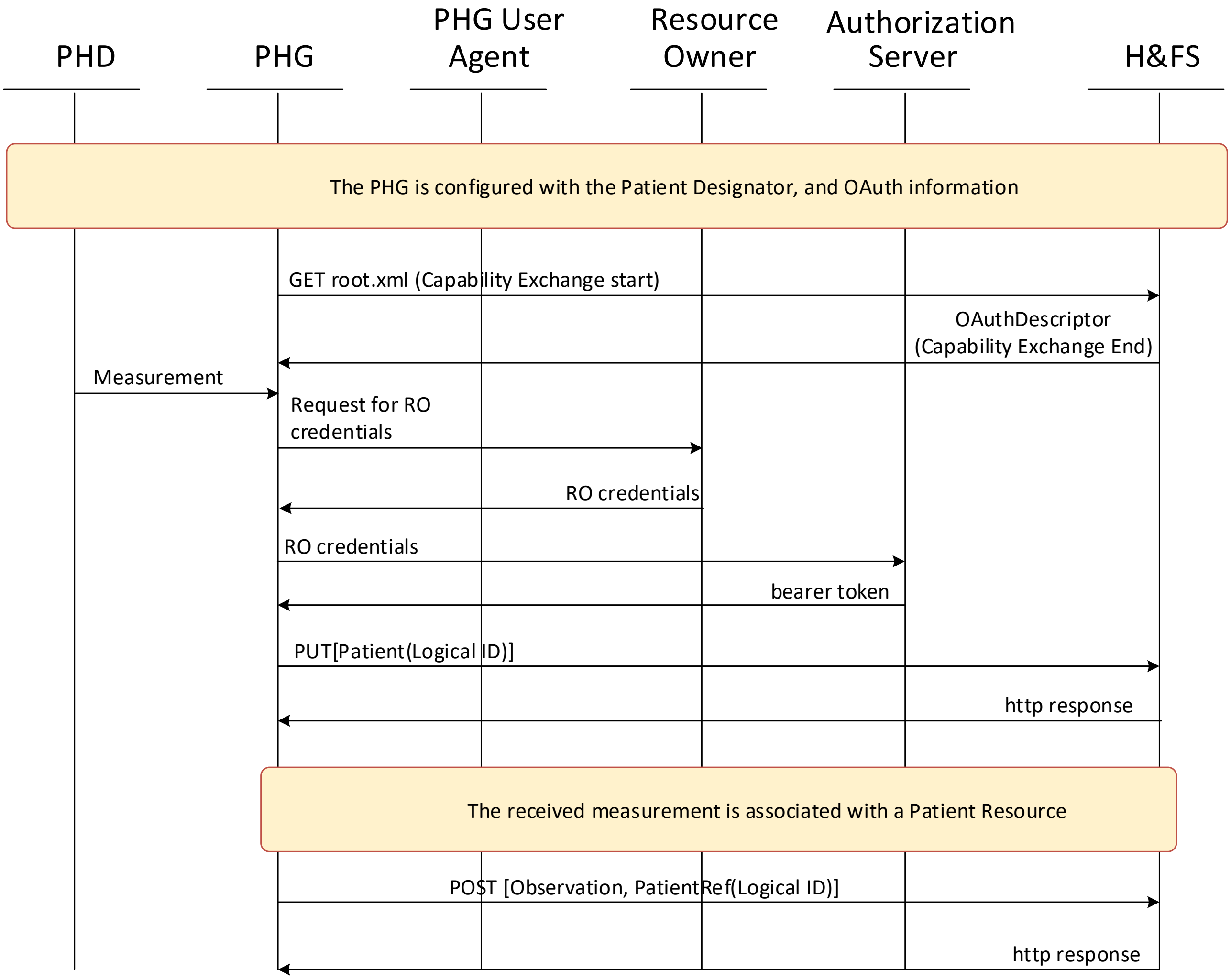
PHD
PHG
PHG User Agent
Resource Owner
Authorization Server
H&FS
The PHG is configured with the Patient Designator, and OAuth information
GET root.xml (Capability Exchange start)
OAuthDescriptor (Capability Exchange End)
Measurement
Request for RO credentials
RO credentials
RO credentials
bearer token
PUT[Patient(Logical ID)]
http response
The received measurement is associated with a Patient Resource
POST [Observation, PatientRef(Logical ID)]
http response

Figure 7-2 – Scenario #2 sequence diagram

7.2.3 Scenario #3

1. The H&FS is configured with a Patient Resource, generating a FHIR Logical ID.

2. The PHG is loaded with the Patient Designator, the H&FS URLs, the client id, the resource owner id, and the password.

3. The PHG performs Capability Exchange with the H&FS to discover the H&FS FHIR upload capabilities.

4. The PHG recognizes that it does not have a valid access token or refresh token. The PHG sends a resource owner grant request to the OAuth authorization server's token endpoint which includes the client id, the resource owner credentials, and the scope.

5. The Authentication Server validates the credentials in the context of the scope and sends an authorization grant in the form of a bearer token.

6. A measurement is taken on the health sensor; the sensor communicates the measurement to the PHG.

7. The PHG receives the measurement and associates the measurement with a patient.

8. The PHG creates the necessary FHIR resources from the received sensor measurement and internal PHG data.

9. The PHG retrieves the Patient Resource from the H&FS using the Patient Designator information and extracts the Patient Resource Logical ID.

10. The PHG uses the Patient Resource Logical ID in building the Observation Resource. These resources are uploaded to the URL obtained from the Capability Exchange Process.

11. The H&FS validates the authorization using the bearer token, and if access is granted stores the FHIR Observation Resource in the context identified by the Patient Resource Logical ID.

12. The H&FS server returns the appropriate HTTP response.

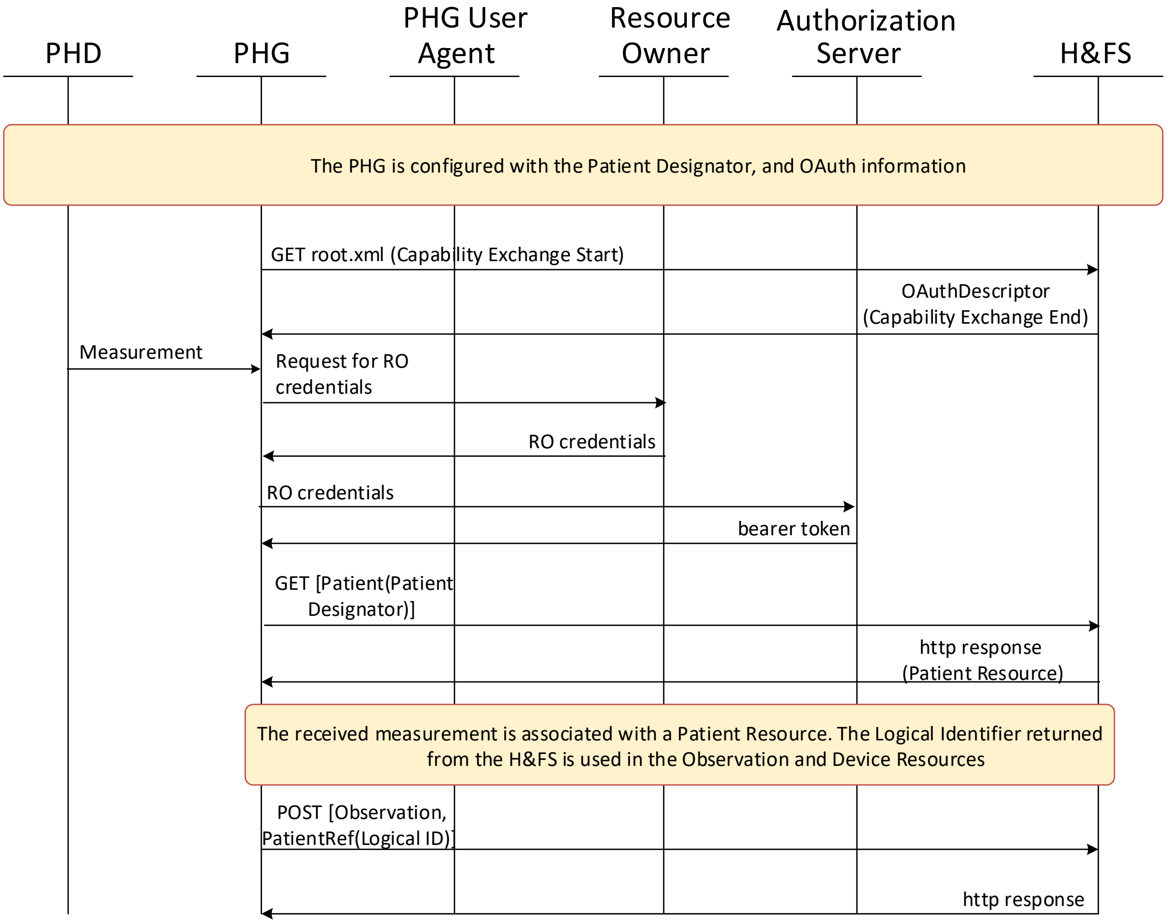
PHD
PHG
PHG User Agent
Resource Owner
Authorization Server
H&FS
The PHG is configured with the Patient Designator, and OAuth information
GET root.xml (Capability Exchange Start)
OAuthDescriptor (Capability Exchange End)
Measurement
Request for RO credentials
RO credentials
RO credentials
bearer token
GET [Patient(Patient Designator)]
http response (Patient Resource)
The received measurement is associated with a Patient Resource. The Logical Identifier returned from the H&FS is used in the Observation and Device Resources
POST [Observation, PatientRef(Logical ID)]
http response

Figure 7-3 – Scenario #3 sequence diagram

7.2.4 Scenario #4

1. The H&FS is configured with a Patient Resource, generating a FHIR Logical ID. An authorized scope is established in which there is only one FHIR patient resource.

2. The PHG is loaded with the H&FS URLs, the client id, the resource owner id, and the password.

3. The PHG performs Capability Exchange with the H&FS to discover the H&FS FHIR upload capabilities.

4. The PHG recognizes that it does not have a valid access token or refresh token. The PHG sends a resource owner grant request to the OAuth authorization server's token endpoint which includes the client id, the resource owner credentials, and the scope.

5. The Authentication Server validates the credentials in the context of the scope and sends an authorization grant in the form of a bearer token.

6. A measurement is taken on the health sensor; the sensor communicates the measurement to the PHG.
7. The PHG receives the measurement and associates the measurement with a patient.
8. The PHG creates the necessary FHIR resources from the received sensor measurement and internal PHG data.
9. The PHG retrieves the available Patient Resource from the H&FS based on its authorized scope of access and extracts the Patient Resource Logical ID.
10. The PHG uses the Patient Resource Logical ID in building the Observation Resource. These resources are uploaded to the URL obtained from the Capability Exchange Process.
11. The H&FS validates the authorization using the bearer token, and if access is granted stores the FHIR Observation Resource in the context identified by the Patient Resource Logical ID.
12. The H&FS server returns the appropriate HTTP response.

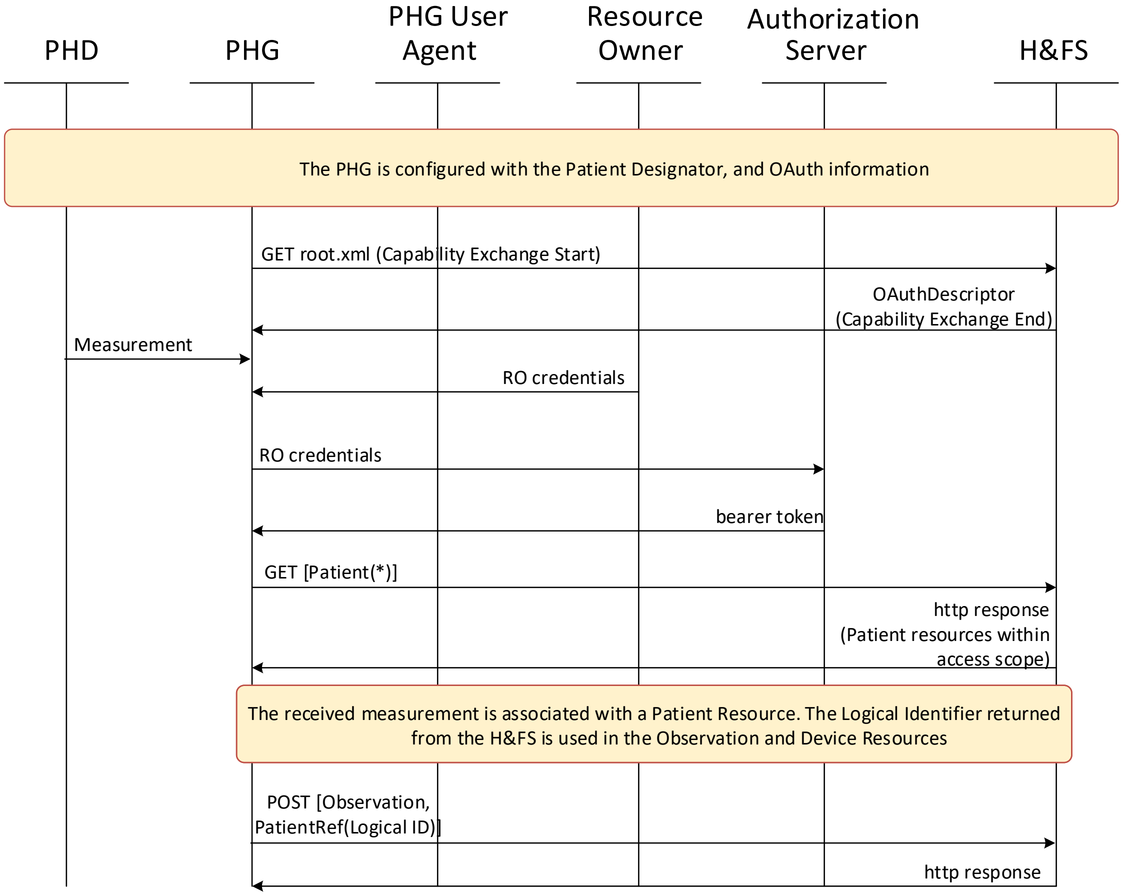
PHD
PHG
PHG User Agent
Resource Owner
Authorization Server
H&FS
The PHG is configured with the Patient Designator, and OAuth information
GET root.xml (Capability Exchange Start)
OAuthDescriptor (Capability Exchange End)
Measurement
RO credentials
RO credentials
bearer token
GET [Patient(*)]
http response (Patient resources within access scope)
The received measurement is associated with a Patient Resource. The Logical Identifier returned from the H&FS is used in the Observation and Device Resources
POST [Observation, PatientRef(Logical ID)]
http response

Figure 7-4 – Scenario #4 sequence diagram

7.3 Example upload from a FHIR observation reporting client

A PHG supporting only a FHIR Observation Reporting Client, or communicating with a H&FS that only supports a FHIR Observation Reporting Server does not need to obtain a consistent understanding of the patient resource Logical ID. There is, therefore, only one use case to consider, which is a simple upload of a complete measurement in which all the FHIR resources are provided in a single FHIR bundle.

7.3.1 Bundle upload

1. The PHG is loaded with the H&FS URLs, the client id, the resource owner id, and the password.
2. The PHG performs Capability Exchange with the H&FS to discover the H&FS FHIR upload capabilities.
3. The PHG recognizes that it does not have a valid access token or refresh token. The PHG sends a resource owner grant request to the OAuth authorization server's token endpoint which includes the client id, the resource owner credentials, and the scope.
4. The Authentication Server validates the credentials in the context of the scope and sends an authorization grant in the form of a bearer token.
5. A measurement is taken on a Personal Health Device (PHD); the PHD communicates the measurement to the PHG.
6. The PHG receives the measurement and associates the measurement with a patient.
7. The PHG creates the necessary FHIR resources from the received sensor measurement and internal PHG data. The internal PHG data includes the Patient Designator. The created FHIR resources are bundled into a single application level packet data unit.
8. These resources are uploaded to the URL obtained from the Capability Exchange Process.
9. The H&FS validates the authorization using the bearer token, and if access is granted accepts the message
10. The H&FS server returns an HTTP response indicating acceptance or rejection of the message.

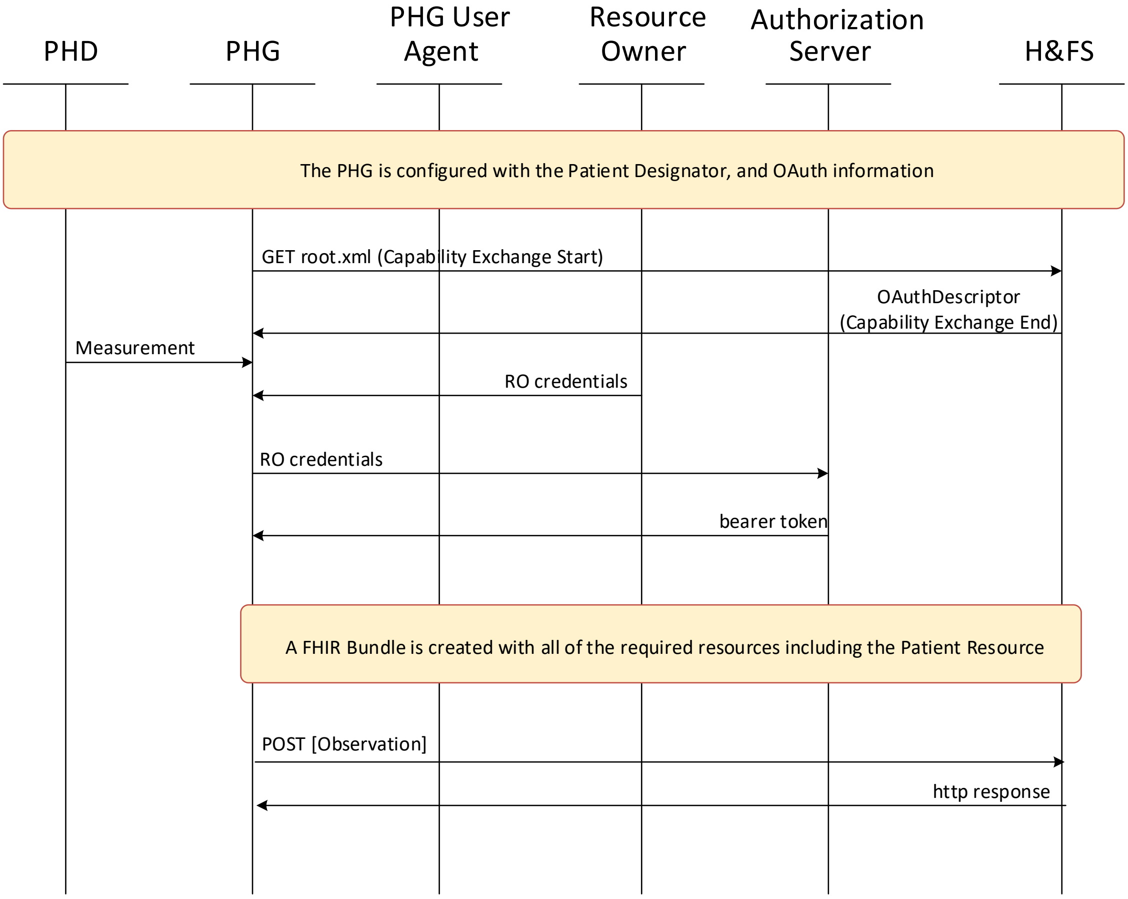
PHD
PHG
PHG User Agent
Resource Owner
Authorization Server
H&FS
The PHG is configured with the Patient Designator, and OAuth information
GET root.xml (Capability Exchange Start)
OAuthDescriptor (Capability Exchange End)
Measurement
RO credentials
RO credentials
bearer token
A FHIR Bundle is created with all of the required resources including the Patient Resource
POST [Observation]
http response

Figure 7-5 – Upload with complete bundle

7.4 Use of JWT

The JSON Web Token Profile for OAuth 2.0 Client Authentication and Authorization Grants [OAuth JWT] can be used to allow a PHG to access resources on a H&FS based on an existing trust relationship without having a direct user-approval step or exposing confidential information to the PHG. To take advantage of the benefits of the JWT, the signing certificate must be loaded onto the PHG. These Guidelines do not proscribe a method by which the PHG is provisioned with a signing certificate. A common pattern, however, is to use a security token service (STS). A STS requires some type of trust relationship with an organization providing the signing certificate, which is typically manifested by the exchange of key material with the STS. WS-Trust [OASIS.WS-Trust] is one available standard for a security token service.

NOTE – If the motivation for using a JWT is to avoid disclosure of a key to the PHG, then the use of an STS may not be desirable as the STS typically requires the PHG to have a key. To address this case, a manual method for configuring the PHG with the JWT is suggested.

8 Behavioural model (Normative)

This clause provides implementation guidelines for conformant operation of a:

– FHIR Observation Server Continua Certified Capability Class

– FHIR Observation Client Continua Certified Capability Class

– FHIR Observation Reporting Server Continua Certified Capability Class

– FHIR Observation Reporting Client Continua Certified Capability Class

In the Continua Architecture, the FHIR clients operate in the context of a PHG and communicate with a FHIR server operating in the context of a H&FS. Exchanges between a PHG and a H&FS take place over the service interface, and the H&FS exposes these capabilities via Capability Exchange.

8.1 Capability exchange

A H&FS with a FHIR Observation Server or a FHIR Observation Reporting Server **shall** implement Capability Exchange as specified in [H.812.3]. The root.xml file for a system supporting a FHIR Observation Reporting Server is the same as the root.xml on a system supporting a FHIR Observation Server, except for the name of the Continua Certified Capability Class. Knowing the supported Continua Certified Capability Class is sufficient for the PHG to properly upload observations.

The OAuthDescriptor is the resource exposed in Capability Exchange that enables the PHG to upload FHIR observations to the H&FS. The OAuthDescriptors on a H&FS are made visible via an Atom Feed in Capability Exchange. A PHG **shall** support Capability Exchange, including the ability to obtain the OAuthDescriptor, as defined in [H.812.3].

The root.xml file for a FHIR Observation Reporting Server is given in Figure 8-1.

```
<profile>
  <!—The location of the document (HCP) describing this profile -->
  <id>FHIR-Observation-Reporting-Server-4C</id>
  <reference>
    http://handle.itu.int/11.1002/3000/hdata/fhir/2017/01/h.812.5.pdf
  </reference>
</profile>
<resourceType>
  <resourceTypeID>OAuthDescriptor</resourceTypeID>
  <!—reference document for OAuthDescriptor  -->
  <reference>
    http://handle.itu.int/11.1002/3000/hdata/fhir/2017/01/h.812.5.pdf
  </reference>
  <representation>
    <mediaType>application/json</mediaType>
  </representation>
</resourceType>
<section>
  <!—Relative path to OAuthDescriptor resource -->
  <path>atom feed/of/OAuthOAuthDescriptor</path>
  <profileID>FHIR-Observation-Reporting-Server-4C</profileID>
  <resourceTypeID>OAuthDescriptor</resourceTypeID>
  <resourcePrefix>true</resourcePrefix>
</section>
```

Figure 8-1 – root.xml components for a FHIR observation reporting server

The root.xml file for a FHIR Observation Server is given in Figure 8-2.

```
<profile>
  <!—The location of the document (HCP) describing this profile -->
  <id>FHIR-Observation-Server-4C</id>
  <reference>
    http://handle.itu.int/11.1002/3000/hdata/fhir/2017/01/h.812.5.pdf
  </reference>
</profile>

<resourceType>
  <resourceTypeID>OAuthDescriptor</resourceTypeID>
  <!—reference document for OAuthDescriptor  -->
  <reference>
    http://handle.itu.int/11.1002/3000/hdata/fhir/2017/01/h.812.5.pdf
  </reference>
  <representation>
    <mediaType>application/json</mediaType>
  </representation>
</resourceType>

<section>
  <!—Relative path to OAuthDescriptor resource -->
  <path>atom feed/of/OauthOauthDescriptor</path>
  <profileID>FHIR-Observation-Server-4C</profileID>
  <resourceTypeID>OAuthDescriptor</resourceTypeID>
  <resourcePrefix>true</resourcePrefix>
</section>
```

Figure 8-2 – root.xml components for a FHIR observation server

The Atom Feed for the OAuthDescriptor, shown in Figure 8-3, applies to both servers.

```
<?xml version="1.0" encoding="UTF-8" ?>
    <feed>
        <title>H.812.5 OAuthDescriptor Resource</title>
        <link rel="self" href="https://dev1.pcha.com/pchaFhir/hData" />
        <author>
            <name>CODE for Healthcare</name>
        </author>
        <id>https://dev1.pcha.com/pchaFhir/hData</id>
        <updated>2017-03-03T00:22:02Z</updated>
        <entry>
            <title>CODE for Healthcare OAuthDescriptor</title>
            <link rel="alternate"
                  href="https://dev1.pcha.com/pchaFhir/hData/@1" />
            <id>https://dev1.pcha.com/pchaFhir/hData/@1</id>
            <updated>2017-06-03T00:22:02Z</updated>
            <summary type="text">OAuthDescriptor</summary>
        </entry>
     </feed>
```

Figure 8-3 – Atom feed for OAuthDescriptor

A H&FS with a FHIR Observation Reporting Server or a FHIR Observation Server **shall** provide the OAuthDescriptor in JSON or XML format, and **shall** set the value of <mediaType> element in the <resourceType> element for a OAuthDescriptor to either application/json or application/xml based on the representation used.

8.1.1 OAuthDescriptor

The OAuthDescriptor is a resource passed from the H&FS to the PHG during CapabilityExchange. The informational content of the OAuthDescriptor allows the H&FS to provide configuration information to the PHG which simplifies the user experience.

Table 8-1 – Elements of the OAuthDescriptor resource provided by H&FS application

Element	Usage
resourceServerURL	The resourceServerURL is the endpoint where the H&FS expects to receive measurements from the PHG. This element **shall** be present
authorizationEndpointURL	The Authorization server's authorizationEndpointURL is the OAuth endpoint the H&FS expects the PHG to use for OAuth authorization. This element **may** be present
tokenEndpointURL	The tokenEndpointURL is the OAuth endpoint the H&FS expects the PHG to use for obtaining the access bearer token. This element **shall** be present
grantTypes	The grantTypes element in the OAuthDescriptor **shall** contain a list of one or more strings selected from the following: "clientCredential", "resourceOwnerCredential", "implicit", "authorizationCode", "rfc7523". The grantTypes element **shall** be present in the OAuthDescriptor.

An example JSON OAuthDescriptor resource is shown in Figure 8-4.

```
{
    "grantTypes": ["resourceOwnerCredential", "rfc7523"],
    "tokenEndPointURL": "http://handle.itu.int/11.1002/3000/hdata/fhir/oauth/token",
    "resourceServerURL": "http://handle.itu.int/11.1002/3000/hdata/fhir/receiver"
}
```

Figure 8-4 – An example JSON OAuthDescriptor resource

8.2 OAuth usage

This clause provides guidance on the use of OAuth for enabling authorized uploads of device measurements from a PHG to a H&FS. The intent of this clause is to provide sufficient specification, that when properly configured, a PHG that supports one of the Continua Certified Capability Classes defined herein for a PHG **shall** be able to securely upload measurements to a Health and Fitness Service that supports either the FHIR Observation Server or the FHIR Observation Reporting Server.

8.2.1 OAuth support

All Continua Certified Capability Classes defined herein **shall** support [OAuth 2.0].

8.2.2 Authorization grants

To foster interoperability this guideline document profiles the use of OAuth authorization grant types. There are five authorization grant types and their typical usage is summarized in Table 8-2.

Table 8-2 – Authorization grant usage

Authorization Grant Type	Typical Usage
client credentials	The trust relationship is with the application itself. The security credentials are known to the PHG application and are independent of the resource owner (user) of the application.
resource owner credentials	The trust relationship is with a resource owner. The security credentials may be provided by the user of the software through a UI, or via a provisioning or configuration process. The security credentials are exposed to the PHG application. Resource Owner credential could be used with a PHG that does not directly interact with a user.
authorization code	The trust relationship is with a resource owner. The PHG application does not gain access to the security credentials. The resource owner needs to be involved in the workflow.
implicit	The trust relationship is with a resource owner. The PHG application does not gain access to the security credentials. The resource owner needs to be involved in the workflow. Similar to authorization code except designed for use with JavaScript based clients in web browsers.
Extension grant (urn:ietf:params:oauth:grant-type:jwt-bearer)	Allows a security certificate to be used on a PHG. Security certificates may provide a better mechanism to manage security credentials as compared to a username/password-based schemes.

A PHG **shall** support the use of one or more of the following OAuth authorization grant types:

– Resource Owner Credentials

– Client Credentials

The PHG **may** support the use of authorization code and implicit grant types.

Additionally, the PHG **may** also support the use of the extension grant with a grant_type value of: "urn:ietf:params:oauth:grant-type:jwt-bearer". This grant type is used when the PHG supports *JSON*

Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [OAuth JWT].

A PHG can use a JWT authorization grant type when it is more desirable to distribute a certificate.

If a PHG specifies a grant_type value of "urn:ietf:params:oauth:grant-type:jwt-bearer" it **shall** conform to the requirements of [OAuth JWT].

A H&FS **shall** support each of the following Authorization Grant types:

– Resource Owner Credential

– Client Credentials

If the H&FS is intended to be used with platforms that support web or interactive interfaces it **shall** support the Authorization Code and implicit grant type.

Additionally, the H&FS **may** support the use of *JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants* [OAuth JWT]. If the H&FS supports *JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants* it **shall** indicate this in Capability Exchange by including the value "rfc7523" for the grantTypes.

8.2.3 Client registration

How a PHG's OAuth client registers with the authentication endpoint as defined in [OAuth 2.0] is out of scope.

8.2.4 Credential distribution

This document does not specify the manner by which resource owner or client credentials are obtained by the PHG. This is considered to be a product specific decision.

OAuth does not define how a resource owner is authenticated, it only addresses authorization. This document also leaves authentication up to the implementation.

8.2.5 Access token scope

This document does not place a requirement on how the scope parameter is to be used.

8.2.6 Authorization using a JSON Web token

8.2.6.1 Introduction

This CDG profiles RFC 7523 [OAuth JWT] to enable the use of a JSON Web Token (JWT) in an OAuth exchange with the token endpoint of an OAuth server. The use of a JWT allows a client to express an existing trust relationship via a credential based mechanism, in which there is no direct user-approval step at the authorization server. The use of a JWT provides an alternative to passwords which may simplify security credential management.

NOTE – The profiling of JWT as a client authentication mechanism, which is also defined in RFC 7523, is out of scope.

8.2.6.2 Transporting assertions in JWTs

A PHG using a JWT to communicate assertions to a H&FS **shall** perform an HTTP POST to the token endpoint as defined in section 4 of [OAuth Assertion] as profiled below:

– The value of grant_type **shall** be "urn:ietf:params:oauth:grant-type:jwt-bearer".

– The assertion parameter **shall** contain a single JWT as specified in [OAuth JWT]

A H&FS returning an error parameter for an invalid JWT **shall** provide additional information regarding the error by using the "error_description" or "error_uri" parameters.

8.2.6.3 JWT claims

A PHG using a JWT **shall** issue the JWT with claims as specified in clause 3 of [OAuth JWT], the PHG is required to meet the following additional requirements

- The JWT **shall** contain an "iat" (issued at) claim that identifies the time at which the claim was issued.
- The JWT **shall** contain a "jti" (JWT ID) claim that provides a unique identifier for the token.

A H&FS that advertises support for JWT in Capability Exchange **shall** conform to the requirements in [OAuth JWT].

8.3 FHIR operations

This clause provides guidelines that profile the behaviour of the PHG and H&FS to ensure that the semantic content of an upload is consistent between all conformant implementations of PHG and H&FS.

8.3.1 Implementation types and interoperability

Conformant H&FSs and PHGs interoperate with each other as shown in Table 8-3.

Table 8-3 – Measurement upload support

	FHIR observation server	FHIR observation reporting server
FHIR Observation Client	Yes [1]	No [2]
FHIR Observation Reporting Client	Yes	Yes

NOTES

[1] – Can upload measurements in an optimized manner

[2] – A given implementation of a FHIR Observation Client might send measurements as complete transaction bundles when it detects a H&FS with a FHIR Observation Reporting Server, but these Guidelines do not require that behaviour.

A FHIR Observation Client can upload to a FHIR Observation Server in an optimized fashion. However, it may not be able to upload to a FHIR Observation Reporting Server at all.

A FHIR Observation Reporting Client will be able to upload to either type of FHIR H&FS; however, it may not take full advantage of the capabilities of a FHIR Observation Server resulting in greater bandwidth consumption.

8.3.1.1 FHIR API support for FHIR observation server

A FHIR Observation Server **shall** support, at minimum, the following FHIR operations as defined by [RESTful FHIR]:

- Instance Level Interactions
  - Update, including conditional update
- Type Level Interactions
  - create, including conditional create
  - search
- Whole System Interactions
  - capabilities
  - transactions

Within a transaction bundle, the following interactions **shall** be supported:

- Instance Level Interactions
  - Update, including conditional update
- Type Level Interactions
  - create, including conditional create

8.3.1.2 FHIR API support for FHIR observation reporting server

A FHIR Observation Reporting Server **shall** support the FHIR *create* call (http POST) of a syntactically correct FHIR transaction bundle as specified by [RESTful FHIR] in which all references can be resolved to resources in the bundle (complete FHIR bundle).

NOTE – Within the transaction bundle additional FHIR operations are allowed (see clause 8.3.1.1), the H&FS **shall not** return an error if the operations specified within the bundle are one of the supported operations for a transaction bundle as identified in clause 8.3.1.1.

8.3.1.3 Obtaining FHIR measurement server type

The PHG **shall** use Capability Exchange to determine the type of measurement receiver.

8.3.2 Measurement uploads

There are three FHIR defined resources that are associated with a measurement upload, the Patient Resource, the Device Resource, and the Observation Resource. These guidelines do not address the behaviour or semantic content of any other FHIR resource.

8.3.2.1 Patient resource

The Patient Resource links the measurement information to the patient. The Logical ID of the Patient Resource identifies the Patient Resource, and indirectly the patient. The PHG must know the Logical ID of the Patient Resource, or must be able to provide a Patient Designator which will allow the Logical ID to be located. Uploading to a FHIR Observation Server.

8.3.2.1.1 Uploading to a FHIR observation server

Clauses 6.1.1 through 6.1.4 cover four anticipated work flows allowing a PHG to upload a Patient Resource to a FHIR Observation Server properly. Within these workflows there are two basic situations, one where the PHG is required to generate the Logical ID of the Patient Resource (scenario 2), and one where it is not (scenarios 1, 3 and 4). When the PHG generates the Logical ID, it must be unique across all Patient Resources within an H&FS defined scope. When the PHG does not generate the Logical ID, it must provide a Logical ID that is known to the H&FS, or use the Patient Designator information to allow the H&FS to locate or create the Logical ID of the Patient Resource, or use a temporary id in the context of a transaction Bundle to obtain the Logical ID.

If a PHG is provided with the Logical ID of the Patient Resource for a given patient, the FHIR Observation Server is indicating that it already has that Patient Resource. In this case the PHG **shall not** upload (FHIR create, conditional create, or update operation) a Patient Resource to the H&FS.

If the Sending PHG is not provided with the Logical ID of a Patient Resource, the PHG will have to have Patient Designator information, which is the information that will allow the PHG to provide values for the *Patient.identifier.system* and *Patient.identifier.value* in the Patient Resource. The *Patient.identifier.type.coding.system* is required to be http://terminology.hl7.org/CodeSystem/v2-0203 and the *Patient.identifier.type.coding.code* element will designate the type of identifier being used in the system and value elements, for example "MR" (Medical Record).

8.3.2.1.2 Patient record logical ID management

When a FHIR Observation Client uploads a Patient Resource using a FHIR *update* operation, the server uses the Logical ID specified by the FHIR Observation Client. When the Patient Resource upload operation is a *create* or a *conditional create*, the Logical ID is created by the H&FS.

- A FHIR Observation Client **shall not** upload a Patient Resource at all if the Patient Logical ID is provided by the service provider.
- A FHIR Observation Client **shall not** specify the Logical ID for the Patient Resource when performing a single-resource create or a conditional create. The FHIR Observation Client **shall** provide the Patient Designator information in the Patient Resource.
- A FHIR ObservationClient **shall** specify the Logical ID for the Patient Resource when performing a single-resource update or when specifying an update transaction for the Patient resource in a transaction Bundle.
- A FHIR Observation [or Reporting] Client **shall** specify a temporary Logical ID for the Patient Resource being created or conditionally created in a Transaction Bundle if the Patient Resource is referenced by another resource in the transaction Bundle. The FHIR Observation [or Reporting] Client **shall** provide the Patient Designator information in the Patient Resource.

8.3.2.1.3 Uploading to a FHIR observation reporting Server

When uploading to a FHIR Observation Reporting Server the measurement **shall** be uploaded as a http POST operation with the payload containing a complete FHIR transaction bundle. Within the transaction bundle the FHIR operation on the Patient Resource **shall** be either update or conditional create.

8.3.2.1.4 Generation of the patient resource

If the PHG needs to generate the Patient Resource, the PHG **shall** follow the mapping specified in the [HL7 FHIR IG].

If the Patient Resource Logical ID is to be created by the PHG the PHG **shall** specify the Logical ID as the concatenation of field values:

Patient.identifier.value-Patient.identifier.system

Where the italicized strings represent the values associated with the named fields, and the "-" is a hyphen character. If this string is longer than 64 characters, it **shall** be truncated to 64 characters by removing characters from the end of the string; the logical id is restricted to 64 characters by FHIR.

If this string contains any characters other than A-Z, a-z, 0-9, "-", or ".", they **shall** be replaced by a "." (period). The PHG is responsible for assuring that the Logical ID is unique.

If the Patient Resource is to be uploaded using a create or conditional create, a logical id **shall not** be specified unless it is temporary id in the context of a transaction Bundle. In the conditional create transaction the “ifNoneExist” parameter **shall** be the health care identification system and the patient identifier placed in the Patient.identifier element as specified above. The client obtains the server generated logical id in the response.

An example of a Patient Resource for an update transaction that is consistent with the patient identifier information in a PCD-01 observation upload is shown in Figure 8-5.

```
"resource":{
    "resourceType":"Patient",
    "meta":{
        "profile":
            "http://hl7.org/fhir/uv/phd/StructureDefinition/PhdPatient"
    }
    "id":"234987sisId-1.2.3.4.5.6.7.8.10",
    "identifier":[
    {
        "type":
        {
            "coding":[
            {
                "system":"http://hl7.org/fhir/v2/0203",
                "code":"MR"
            } ]
        },
        "system":"urn:oid:1.2.3.4.5.6.7.8.10",
        "value":"234987sisId"
    } ],
    "name":[
    {
        "family":["Longstrump"],
        "given":["Pippi","Ulla"]
    }
}
```

Figure 8-5 – An example of Patient Resource update transaction

8.3.2.2 Device resource

When a Device Resource is uploaded as a single resource or in a bundle the PHG **shall** use the FHIR update or conditional create operations. The Logical ID of the Device Resource **shall** be unique on the H&Fs. If an update transaction is specified, the PHG needs to assure that the Logical ID is unique. A transport address, system id value, or a combination of the two are options. If neither of these fields are available, a UUID can be used.

8.3.2.3 Observation resource

When an Observation Resource is uploaded, either as a single resource or in a bundle, the PHG **shall** use the create or conditional create operations.

8.3.2.3.1 Duplicate observations

Personal Health Devices (PHD) often store data locally, allowing the device to be used while not in range of a PHG. Not all devices that store local data delete the data after delivering it to the PHG. This non-removal of duplicate data can lead to duplicate data being pushed into the Continua ecosystem.

The PHG **should** attempt to filter out duplicate data when sending device measurements to a H&FS.

A PHG **should** filter out duplicate measurements from the sensor device(s) using an implementation defined filtering algorithm.

Once the received measurements have passed through the duplicate filtering process, a PHG **shall** use a conditional create to upload the measurement unless one or more of the following conditions are true, in which case a create is used:

– The measurement is received by the PHG and there is no associated timestamp for the measurement.

– The measurement received by the PHG is a live measurement. The PHG **shall** identify a live measurement based on the difference between the time of reception of the measurement, and the corrected timestamp provided by the PHD. If the corrected timestamp indicates that the measurement was taken by the PHD within an application defined expiration period, then the measurement is considered to be live. These guidelines do not proscribe a value for the expiration period as it depends on the sensor itself, and the way the sensor is used. A suggested value for the expiration period is sixty (60) seconds.

8.3.2.4 Payload format

A PHG **shall** use either JSON or XML when uploading a measurement. A H&FS **shall** support uploads in JSON format and **may** support uploads in XML format.

9 Normative guidelines

The tables in this clause list the guidelines for the four Continua Certified Capability Classes associated with uploading a device observation using FHIR.

9.1 Requirements common to both H&FS FHIR capability classes

This clause addresses the conformance requirements that are common to both the FHIR Observation Server and the FHIR Observation Reporting Server. The term H&FS is used to designate both the FHIR Observation Reporting Server and the FHIR Observation Server.

Table 9-1 – Requirements common to both H&FS FHIR capability classes

Name	Description	Comments
FHIR-H&FS-oauth-2.0-required	A H&FS **shall** support [OAuth 2.0]	
FHIR-H&FS-oauth-grantTypes	A H&FS **shall** support the following Authorization Grant types: – Resource Owner Credential – Client Credentials	Other grant types may also be supported
FHIR-H&FS-oauth-grantTypes-interactive-grants	A H&FS **shall** conditionally support the Authorization Code and implicit grant type if the H&FS is intended to be used with platforms that support web or interactive interfaces.	Conditional support is determined by developer
FHIR-H&FS-CE-supported	A H&FS with a FHIR Observation Server or a FHIR Observation Reporting Server **shall** implement Capability Exchange as specified in [H.812.3].	A Continua H&FS simplifies provisioning of PHGs through Capability Exchange. Non Continua FHIR servers may require other means to obtain provisioning information.

Name	Description	Comments
FHIR-H&FS-CE-HCP-reference	The value of the <reference> child element in the <profile> element of the root.xml file, which points to the Hdata Content Profile document, **shall** point to the latest revision of this document that the implementation supports.	The resource at the provided URL is what determines the latest supported version.
FHIR-H&FS-CE-resourceType	A <resourceType> element with a <resourceTypeID> child element set to the value OAuthDescriptor **shall** be present in the root.xml file.	
FHIR-H&FS-CE-resourceType-reference	The <reference> element for the resourceType **shall** point to the latest revision of this document that the implementation supports.	
FHIR-H&FS-CE-resourceType-representation	The <mediaType> element in the <representation> element for the resourceType **shall** be set to application/json or application/xml.	
FHIR-H&FS-CE-resourceType-consistency-xml	If the mediaType is set to application/xml the H&FS **shall** use XML to represent Capability Exchange information as defined in [H.812.3] or return an error indicating that it does not support XML.	
FHIR-H&FS-CE-resourceType-consistency-json	If the mediaType is set to application/json the H&FS **shall** use JSON to represent Capability Exchange information as defined in [H.812.3].	
FHIR-H&FS-CE-section-resourceTypeID	The <resourceTypeID> element in the section **shall** be set to OAuthDescriptor.	
FHIR-H&FS-CE-section-atom-feed	When the base path is concatenated as a prefix to the contents of the <path> child element in the <section> element, the H&FS **shall** return an atom feed that lists the OAuthDescriptor resources.	
FHIR-H&FS-CE-OAuthDescriptor-entries	The H&FS **shall** provide a OAuthDescriptor for each distinct FHIR uploading service it exposes.	
FHIR-H&FS-CE-section-not-empty	The atom feed returned by H&FS **shall** have at least one OAuthDescriptor listed.	
FHIR-H&FS-OAuthDescriptor	The H&FS **shall** return an OAuthDescriptor as specified in Table 8-1.	There are multiple conformance requirements in referenced table
FHIR-H&FS-RFC7523	A H&FS **may** include the "rfc7523" string in the grantTypes element of the OAuthDescriptor. If it does it **shall** conform to the requirements of IETF RFC 7523.	

Name	Description	Comments
FHIR-H&FS-RFC7523-invalid-jwt	A H&FS returning an error parameter for an invalid JWT **shall** provide additional information regarding the error by using the "error_description" or "error_uri" parameters.	
FHIR-H&FS-no-error-bundle	For a syntactically correct transaction bundle in which there are no external references the H&FS **shall not** return an http error due to unsupported FHIR operations.	
FHIR-H&FS-xml-and-json-support	A H&FS **shall** support uploads in both JSON format. It **may** support uploads in XML format.	
FHIR-H&FS-OPS-API-Create	A H&FS **shall** support the FHIR create API call (http POST) of a syntactically correct FHIR transaction bundle as specified by [RESTful FHIR] in which all references can be resolved to resources in the bundle (complete FHIR bundle).	

9.2 Requirements common to both PHG FHIR capability classes

This clause addresses the conformance requirements that are common to both the FHIR Observation Client and the FHIR Observation Reporting Client, which are listed in Table 9-2. To simplify description within this table, the term PHG is to be understood to represent both the FHIR Observation Client and FHIR Observation Reporting Client Continua Certified Capability Classes.

Table 9-2 – Requirements common to both PHG FHIR capability classes

Name	Description	Comments
FHIR-PHG-oauth-2.0-required	A PHG implementing the FHIR-Observation-Uploader **shall** support [OAuth 2.0]	
FHIR-PHG-oauth-grantTypes	A PHG **shall** support the use of one or more of the following OAuth Authorization Grant types: – Resource Owner Credentials – Client Credentials – Authorization Code – Implicit	
FHIR-PHG-conditional-rfc7523-support	A PHG **may** send a grant_type value of: "urn:ietf:params:oauth:grant-type:jwt-bearer" to an H&FS that has the 'rfc7523' value in the grantTypes element of the OAuthDescriptor. If it does, it **shall** conform to the requirements of RFC 7523.	

Name	Description	Comments
FHIR-PHG-use-of-rfc7523	A PHG **shall not** send a grant_type value of: "urn:ietf:params:oauth:grant-type:jwt-bearer" to an H&FS that does not list the 'rfc7523' value in the grantType element of the OAuthDescriptor	
FHIR-PHG-rfc7523-jwt-bearer	A PHG using a bearer JWT as defined in [OAuth JWT] **shall** issue an access token request as defined in section 4 of [OAuth Assertion] with the following parameters and values: – grant_type **shall** be "urn:ietf:params:oauth:grant-type:jwt-bearer". – assertion **shall** contain a single JWT	
FHIR-PHG-rfc7523-claims	A PHG using a JWT **shall** issue the JWT with claims as specified in clause 3 of [OAuth JWT].	
FHIR-PHG-rfc7523-claims-iat	The JWT **shall** contain an "iat" (issued at) claim that identifies the time at which the claim was issued	
FHIR-PHG-rfc7523-claims-jti	The JWT **shall** contain a "jti" (JWT ID) claim that provides a unique identifier for the token.	
FHIR-PHG-discover-server-type	A PHG **shall** have an implementation of Capability Exchange that conforms to [H.812.3] including the Atom Feed to enable access to the OAuthDescriptor	A PHG implementation must provide a way to use Capability Exchange to obtain the OAuthDescriptor of a H&FS.
FHIR-PHG-FOS-patient-resource-no-upload	If the PHG is provided the Logical ID of the Patient Resource, the PHG **shall not** upload a Patient Resource to the H&FS.	Applies when uploading to a FHIR Observation Server
FHIR-PHG-patient-resource-no-logical-id-on-creates	A PHG **shall not** specify the Logical ID for the Patient Resource when performing a single-resource create or a conditional create of the Patient Resource. The PHG **shall** provide the Patient Designator information in the Patient Resource.	
FHIR-PHG-patient-resource-logical-id-on-update	A PHG **shall** specify the Logical ID for the Patient Resource when performing a single-resource update.	
FHIR-PHG-patient-resource-temporary-logical-id	A PHG **shall** specify a temporary Logical ID for the Patient Resource being created or conditionally created in a Transaction Bundle if the Patient Resource is referenced by another resource in the transaction Bundle. The PHG **shall** provide the Patient Designator information in the Patient Resource.	

Name	Description	Comments
FHIR-PHG-FORS-upload-complete-bundle-using-post	When uploading to a FHIR Observation Reporting Server the measurement **shall** be uploaded as a http POST operation with the payload containing a complete FHIR transaction bundle.	
FHIR-PHG-FORS-upload-complete-bundle-ops	Within a transaction bundle the FHIR operation on the Patient Resource **shall** be either update or conditional create. The update **shall only** be used when the Logical ID of the Patient Resource is known.	
FHIR-PHG-patient-resource-gen-pid-structure	If the Patient Resource Logical ID is to be created by the PHG the PHG **shall** specify the Logical ID as the concatenation of field values: *Patient.identifier.value-Patient.identifier.system* Where the italicized strings represent the values associated with the named fields, and the "-"is a hyphen character. If this string is longer than 64 characters, it **shall** be truncated to 64 characters by removing characters from the end of the string. If this string contains any characters other than A-Z, a-z, 0-9, "-", or ".", they **shall** be replaced by a "." (period).	The PHG is responsible for assuring that the logical id is unique. If it cannot assure uniqueness, for example when the result has to be truncated or characters need to be replaced, it should use another approach such as conditional creates.
FHIR-PHG-patient-resource-upload-conditional-create	If the Patient Resource is to be uploaded using a conditional create, a logical id **shall not** be specified. The “ifNoneExist”parameter **shall** be the health care identification system and the patient identifier placed in the Patient.identifier element as specified above.	
FHIR-PHG- device-upload	When a Device Resource is uploaded as a single resource or in a bundle the PHG **shall** use the FHIR update or conditional create operations.	
FHIR-PHG- device-id	The Logical ID of the DeviceResource **shall** be unique on the H&Fs and **should** contain the IEEE systemId of the device this component is to represent. If the systemId is not available, then the Logical ID **should** be set to a UUID conformant to RFC 4122.	
FHIR-PHG-obsres-upload	When an Observation Resource is uploaded, either as a single resource or in a bundle, the PHG **shall** use the create or conditional create operations.	

Name	Description	Comments
FHIR-PHG-dup-filter	The PHG **should** attempt to filter out duplicate data when sending measurements to a H&FS using an implementation defined filtering algorithm.	
FHIR-PHG-dup-use-of-conditional-create	A PHG **shall** use a conditional create to upload measurement unless one or more of the following conditions are true, in which case a create **shall** be used (1) The measurement is received by the PHG and there is no associated timestamp for the measurement. (2) The measurement received by the PHG is a live measurement.	See clause 8.3.2.3.1 for additional details.
FHIR-PHG-use-of-xml-and-json	A PHG **shall** format measurement payloads in JSON or XML.	
PHG Mapping Requirements		
FHIR-PHG-HL7-IG	PHGs **shall** map PHD and Patient data as specified in the [HL7 FHIR IG].	
FHIR-PHG-Sync-qualified-time	A PHG **shall** be capable of synchronizing to qualified time.	The PHG is to map the sensor time line to qualified time. Qualified time is any time synchronized to UTC with or without knowledge of local time. See the [H.812.1] section on timestamping for additional details.

9.3 Requirements specific to the FHIR observation server

This clause addresses the conformance requirements that are specific to the FHIR Observation Server. Additional requirements apply to this certified capability class, see clause 9.1.

Table 9-3 – Requirements specific to the FHIR observation server

Name	Description	Comments
FOS-CE-profile-id	The value of the child element <id> in the <profile> element **shall** be set to "FHIR-Observation-Server-4C".	
FOS-CE-section-profileID	The value of the child element <profileID> in the <section> element **shall** be set to "FHIR-Observation-Server-4C".	

Name	Description	Comments
FOS-supported-FHIR-operations	A FHIR Observation Server **shall** support, at minimum, the following FHIR operations as defined by [RESTful FHIR]: – Instance Level Interactions o Update – Type Level Interactions o create, including conditional create o search – Whole System Interactions o Capabilities o transactions	

9.4 Requirements specific to the FHIR observation reporting server

This clause addresses the conformance requirements that are specific to the FHIR Observation Reporting Server. Additional requirements apply to this certified capability class, see clause 9.1.

Table 9-4 – Requirements specific to the FHIR observation reporting server

Name	Description	Comments
FORS-CE-profile-id	The value of the child element <id> in the <profile> element **shall** be set to "FHIR-Observation-Reporting-Server-4C"	
FORS-CE-section-profileID	The value of the child element <profileID> in the <section> element **shall** be set to "FHIR-Observation-Reporting-Server-4C".	

9.5 Requirements Specific to the FHIR observation client

This clause addresses the conformance requirements that are specific to the FHIR Observation Client. This CDG does not mandate how a FHIR Observation Client optimizes its measurement uploads with a FHIR Observation Server, however, if the PHG can only send measurements as complete transaction bundles it is considered a FHIR Observation Reporting Client. Additional requirements apply to this certified capability class, see clause 9.2.

Table 9-5 – Requirements specific to the FHIR observation client

Name	Description	Comments
FHIR-FOC-FORS-must-use-bundle	When a H&FS advertises a FHIR Observation Reporting Server the PHG **shall** only send measurements that are fully contained in a complete transaction bundle.	The FOC may upload measurements to a FORS but is not required to do so.

Name	Description	Comments
FHIR-FOC-FOS-optimize-upload	A FHIR Observation Client **should** optimizes its measurement uploads with a FHIR Observation Server by using single resource interactions that avoid repeating data already uploaded	The PHG is responsible for assuring that the logical id is unique. If it cannot assure uniqueness, for example when the result has to be truncated or characters need to be replaced, it should use another approach such as conditional creates.

9.6 Requirements Specific to the FHIR observation reporting client

This clause addresses the conformance requirements that are specific to the FHIR Observation Reporting Client. Additional requirements apply to this certified capability class, see clause 9.2.

Table 9-6 – Requirements specific to the FHIR observation reporting client

Name	Description	Comments
FHIR-FORC-FOS-support	A PHG implementing only a FHIR Observation Reporting Client **shall** be able to upload measurements to a H&FS advertising a FHIR Observation Server Continua Certified Capability Class.	A conformant FOS can handle the FHIR transaction bundle of a FORC. The FORC can therefore deliver the measurement to the FOS successfully
FHIR-FORC-supports-FORS	A PHG claiming support for a FHIR Observation Reporting Client **shall** be able to upload a measurement to a H&FS advertising a FHIR Observation Reporting Server Continua Certified Capability Class.	This is the interoperability baseline

Annex A

ISO/IEEE 11073 to FHIR resource mapping

This Annex has been replaced by [HL7 FHIR IG].

Appendix I

FHIR background

This appendix has been replaced by [HL7 FHIR IG].

Bibliography

See [H.810] for a list of non-normative references and publications that contain further background information.

[HL7.FHIR-API] HL7 FHIR Release 4, RESTful API, http://www.hl7.org/fhir/http.html (visited 2019-10-31)

[HL7-FHIR-MODEL] HL7 FHIR Release 4, Resource index, http://www.hl7.org/fhir/resourcelist.html (visited 2019-10-31)

[H.812.1] ITU-T H.812.1 (2017), *Interoperability design guidelines for personal connected health systems: Services interface: Observation Upload capability*. https://www.itu.int/rec/T-REC-H.812.1

[H.812.3] ITU-T H.812.3 (2017), *Interoperability design guidelines for personal connected health systems: Services interface: Capability Exchange capability*. https://www.itu.int/rec/T-REC-H.812.3

[OAuth 2.0] IETF RFC 6749 (2012), The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749

[OAuth Assertion] IETF RFC 7521 (2015), *Assertion framework for OAuth 2.0 client authentication and authorization Grants*. https://tools.ietf.org/html/rfc7521

[OAuth JWT] IETF RFC 7523 (2015), *JSON Web token (JWT) profile for OAuth 2.0 client authentication and authorization grants*. https://tools.ietf.org/html/rfc7523

[OASIS.WS-Trust] WS-Trust 1.4 (2012), Nadalin, A., Ed., Goodner, M., Ed., Gudgin, M., Ed., Barbir, A., Ed., and H. Granqvist, Ed., "WS-Trust", February 2009, http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html

[ISO/IEEE 20601] ISO/IEEE 11073-20601:2016, Health informatics – Personal health device communication – Part 20601: Application profile – Optimized exchange protocol. http://www.iso.org/iso/catalogue_detail.htm?csnumber=66717. Also available as https://standards.ieee.org/standard/11073-20601-2016.html

[HL7 FHIR IG] Personal Health Device Implementation Guide (0.3.0 STU 1, 2nd ballot, at time of publication). http://build.fhir.org/ig/HL7/PHD (visited 2019-10-31)