CommonWell Health Alliance Specification V4.4

Services (Part 1 of 2)

Revision History – Summary of Changes

V4.4 - Published

- Document Reference Patient Search FHIR Parameter Change to Patient.Identifier
- Updated section 11 Patient Access Data Requests with IAS Provider AAL2 requirements
- Updated section 8.4.1 Get Patient Links with details on how MPI handles matches for multi-part given name
- Updated section 11.1.1.3 TEFCA Individual Access Services for more clarity on supporting v1 and v2 SOP

V4.3 - Published

- Delegation of Authority – Support for CommonWell and Carequality
- IAS – More details about the SAML and JWT included
- Updated Section 10.2 (FHIR) for better clarity on date and period parameters
- Added GET Patient Disclosure to 8.3.5 Patient Disclosure
- Added new section 8.3.6 Event Notification Services
- Link to CommonWell MPI & Patient Matching article added in section 8.4 Patient Identification and Linking
- Changed name cardinality to only accept an array with one string value in 8.4.6 Patient Object
- Added new section 10.2.3 Patient Match for searching and retrieving patient matches with FHIR
- Updated section 10.3 XCA with a table of supported search parameters
- Added new section 10.3.3 Targeted XCA Query

V4.2 – Published

- Added new section 7.6 Delegation of Authority for information on delegated requests
- Added new GET Patient Disclosure endpoint to 8.3.5 Patient Disclosure
- Added new consentToDisclose field to Patient Object
- Changed gender field in Patient Object to optional

V4.1 – Published

- Added Revision History section
- Updated 8.3.2 to reference new alternatePatients field
- Added new section 11.1.1.1 AlternatePatients for validated attributes
- Added new section 11.1.1.3 TEFCA Individual Access Services
- Added new section Appendix A.5 – Mime Types
- Zip code required for patient address and clarified accepted zip format
- Primary “source” patient ID will always have patient.identifier.use = “official”
- Added new field identifier.assigner to the patient object
- Added additional details for how Merge Patient request body
- Updated Patient Discloser method from PUT to POST
- Support new TEFCA codes for T-PH-ECR, T-PH-ELR, T-HCO-CC, T-HCO-HED, T-HCO-QM
- Updated 10.2 with supported FHIR DocumentReference search parameters
- Updated 9.1 to support PD1-12, Protection Indicator, and patient record disclosure
- Return historical addresses for GET Patient Links by Patient ID and GET Probable Links by Patient ID
- Return historical patient names for GET Probable Links by Patient ID
- In the Patient object, support telecom phone numbers between 7-15 digits
- Fixed reference to patient object in section 8.4.6 Patient Object.
- Updated Patient Object to note that required fields are for create/add and that patient matching is in internal documentation.

V4.0 – Published June 5,2024

- Initial version with new Technical Service Provider

1 Foundational Concepts

The CommonWell Health Alliance Specification (hereinafter the "Specification" or "specification") is comprised of Services and Use Cases, collectively the "specification", and defines the approved specifications and detailed technical and interoperability requirements for a compliant implementation of the services offered by the Alliance, that may be consumed by healthcare information system providers for the purpose of exchanging healthcare information over the internet.

1.1 Introduction

The CommonWell Health Alliance Specification (hereinafter the "Specification" or "specification") is comprised of Services (Part 1 of 2) and Use Cases (Part 2 of 2), collectively the "specification", and defines the approved specifications and detailed technical and interoperability requirements for a compliant implementation of the services offered by the Alliance, that may be consumed by healthcare information system providers for the purpose of exchanging healthcare information over the internet.

1.2 Intended Audience

The audience for this specification consists of those responsible for designing and building software systems that will use the CommonWell services. This specification provides a detailed description of the services and how they should be used.

2 Architecture

The services described in this specification establish a common infrastructure to enable health document sharing. The architecture is based on centralized Patient discovery and matching adjudication services. CommonWell also provides document query and retrieval services that incorporate a brokered service acting against a federated network of document registries and repositories.

CommonWell will support a prior version of an API for **at least one year** from the date on which the next major version goes into general release.

2.1 Design Goals and Assumptions

The CommonWell services have the following primary design goals and assumptions:

- Leverage existing standards.
- Provide a centralized service for Patient discovery and record location.
- Provide a brokered service for document query and retrieval.
- Utilize a federated security model for authentication and authorization.
- Audit transactions occur within the CommonWell service boundary.

The CommonWell services will NOT provide the following:

- Will NOT provide centralized document registry or repository services.
- Will NOT provide a centralized ATNA auditing service; systems leveraging the CommonWell services (hereafter referred to as *Edge Systems*) are responsible for auditing events within their respective application domains.

2.2 Integrating the Health Enterprise (IHE) Profiles

The CommonWell services defined in this specification support IHE Integration Profiles as described in the following sections.

2.2.1 Patient Identifier Cross-Referencing (PIX)

The Patient Identifier Cross-Referencing (PIX) (http://wiki.ihe.net/index.php?title=Patient_Identifier_Cross-Referencing) integration profile supports the cross-referencing of Patient Identifiers from multiple Patient Identifier Domains by:

- Transmitting Patient Identity information
- Providing the ability to access the list(s) of cross-referenced Patient Identifiers via a query/response transaction.

The CommonWell service represents an implementation of this profile by establishing a centralized Patient Identifier Cross-reference Manager. An Edge System acts as Patient Identity Source in the context of this profile by providing a Patient Identity Feed to the CommonWell Patient Identifier Cross- reference Manager.

See Section 9 for Implementation details for the CommonWell Patient Identifier Cross Referencing interfaces.

See Appendix B for PIX performance targets agreed upon by the CommonWell Health Alliance.

2.2.2 Cross-Community Access (XCA)

The Cross-Community Access (XCA) integration profile supports the means to query and retrieve patient-relevant medical data held by other communities. A *community* is defined as a coupling of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing health information.

CommonWell represents an XCA community insofar as registered organizations have agreed to share health information. The CommonWell Health Alliance Broker (CHA Broker) service, described in section 10, provides a brokered service for **Find Documents Registry Stored Query/Cross Gateway Query** and **Retrieve Document Set/Cross Gateway Retrieve** transactions as defined in IHE ITI-18, ITI-38, ITI-39 and ITI-43. The CHA Broker will support receiving both XDS.b (ITI-18 and ITI-43) and XCA (ITI-38 and ITI-39) forms of these transactions as specified in the IHE specifications. All communication from the CHA Broker to member responding gateways will be through the XCA query and retrieve transactions. CommonWell also supports REST-based document query and retrieve based on HL7 FHIR resources and their related transactions.

CommonWell member organizations that want to respond to document query & retrieval requests MUST register their respective XCA/FHIR Responding Gateway services. In addition to supporting the required query and retrieve XCA transactions (ITI-38 and ITI-39) or FHIR transactions

(DocumentReference and Binary), the member responding gateway may also support one or both of the two IHE options: On-Demand Documents and Persistence of Retrieved Documents. As a Document Consumer, Edge Systems MUST include the On-Demand Document option as specified in the IHE ITI On-Demand Documents Supplement. This option is necessary to ensure complete retrieval of all patient documentation.

Currently, CommonWell supports the following versions of the IHE specifications for each of these transactions and options:

XCA specifications

- Transaction overview: Integration Profiles, publication date 10/25/2013, Version 10.1 (http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf)
- ITI-18 specification: Transactions Part A, publication date 9/27/2013, Version 10.0 (http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf)
- ITI-38, ITI-39 and ITI-43 specifications: Transactions Part B, publication date 9/27/2013, Version 10 (http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf)

FHIR specifications

- R4
    - US Core DocumentReference Profile
    - Document Reference: Resource DocumentReference v4.0.1
    - Binary: Resource Binary v4.0.1
- On-Demand Documents option:
    - On-Demand Documents, publication date 10/25/2013, Version 1.3 (http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_On_Demand_Documents.pdf)
- Persistence of Retrieved Documents:
    - Transaction overview: Integration Profiles, publication date 10/25/2013, Version 10.1 (http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf)
    - XDS-SD specification: Cross-Transaction Specifications and Content Specifications, publication date 9/27/2013, Version 10.0 (http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf)

CommonWell also has agreements on the set of coding systems and values to be used for document metadata.

Additional information on the following items can be found in the internal SharePoint site, accessible by Service Adopters:

- Approved metadata
- REST-based document query and retrieve operations and mappings to the IHE XDS profile

2.2.3 Cross-Enterprise User Assertion (XUA)

The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate identity information about an authenticated principal (user, application, system) in transactions that cross enterprise boundaries.

The transactions between Edge Systems and CommonWell will use an authorization framework based on Identity Federation standards. These standards support user directories distributed among the various Edge Systems.

As part of the CommonWell-brokered document query and retrieval workflow detailed in this specification, Edge Systems will generate the SAML 2.0 Token and include this token in the SOAP header of the SOAP-based messages exchanged as specified in the Cross-Community Access (XCA) integration profile.

2.3 CommonWell REST-based Services

In addition to the IHE-defined SOAP transactions described above, CommonWell also provides REST services which support workflows facilitating patient management, Patient Record matching, Person Enrollment and Patient discovery. These workflows are enhanced and supported by verification policies and the use of verifiable "strong identifiers" like driver licenses and state-issued identification cards.

2.3.1 Resource Definitions

Following the REST architectural style, the application protocol operations defined in section 8.6.10 of this specification are executed by manipulating the underlying resource representations. Link relations included in the resource representations provide the mechanism for clients to transition the state of a resource in an application workflow.

2.3.2 Fast Healthcare Interoperability Resources (FHIR)

Fast Healthcare Interoperability Resources (FHIR) defines a set of resources for use in exchanging information about the healthcare process. In accordance with the FHIR license, this specification represents a derivative specification and a REST-based implementation and extension of particular FHIR resource definitions.

FHIR resource definitions are still in draft status. However, FHIR is sponsored by HL7 and is derived from both the collective experience of the HL7 membership and wide community feedback from the development and application of a spectrum of healthcare interoperability solutions.

The front-end REST based Services are FHIR R4 and US Core compliant.

2.3.3 Link Relations

To support the hypermedia constraint, link relations associated with resource representations will use the format defined in the Hypertext Application Language (HAL) media type. HAL provides a set of conventions for expressing hyperlinks to related resources and thus avoids the necessity to create a custom media type for the resources defined in this specification.

2.3.4 Resource Format

The supported format for resource representations is JavaScript Object Notation (JSON).

2.3.5 Performance

CommonWell Health Alliance agreed upon performance targets for the REST services are outlined in Appendix B.

3 Conventions Used in this Document

The keywords “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC-2119 [RFC2119] (http://www.ietf.org/rfc/rfc2119.txt).

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

4 Glossary of Terms

This section defines commonly used terms.

Object Identifier (OID)

An OID is a standard identification mechanism for naming any type of object, concept or “thing” with a globally unambiguous, persistent name.

Organization
A healthcare system that interacts with the CommonWell services as a provider of Patient Identity information and as a consumer of the CommonWell Patient discovery and record location services. This term is used interchangeably with Community.

An Organization’s Edge System acts as a source of Patient Record data to CommonWell.
An Organization’s Responding Gateway maintains publicly available service endpoint(s) for query and retrieval of clinical data related to patients maintained by the Organization.
An Organization may represent a single health care facility or a Health Information Exchange (HIE) entity.

Organization ID
Globally unique OID, representing the Organization of the Edge System

Assigning Authority ID
Globally Unique OID, representing patient identity management for the Organization.

Edge System
An Edge System is any healthcare information system that can interact with the CommonWell services. This includes systems that will submit Patient Identity data, can query for Patient Record locations and associated visits, and will perform document query and retrieval.

Visit
A Visit represents an encounter between an individual and a participating Organization for the purpose of providing patient service(s) or assessing the health status of a patient.

Local Patient Record
In the context of interactions between an Edge System and CommonWell, this describes a Patient Record that exists in the local Edge System. This may or may not include encounter information that may be used to assist in match adjudication.

Remote Patient Record
In the context of interactions between a local Edge System and CommonWell, this describes a Patient Record

that exists in an Organization to which the Edge System does not belong.

CommonWell Patient Record

A record stored within CommonWell of Patient demographic, identity and visit information unique to the care setting(s) associated with an Organization.

CommonWell Patient Identifier

The CommonWell Patient Identifier is an object identifier (OID) that represents a unique and unambiguous name for a Patient Record.

The CommonWell Patient Identifier is created by the CommonWell system when processing a Patient Add operation during a Patient Identity Feed transaction and is stored with a CommonWell Patient Record as its Identifier.

To obtain the CommonWell Patient Identifier associated with a Local Patient Record, an Edge System can query CommonWell using the PIX Query transaction or can query CommonWell directly using the REST-based resource representation for a Patient.

This identifier is essential for certain key CommonWell workflows – for example, the CommonWell Patient Identifier MUST be used to refer to a Patient in requests for documents and document metadata as described in the Document Query and Retrieval workflow.

CommonWell Person Record
The CommonWell Person Record is an individual known outside the context of an individual Organization. A Person Record contains general demographic information and may also include one or more validated authoritative identifiers (stored as hashed values). This record is created in the CommonWell system by the Master Person Index (MPI).

As a pre-condition for use of CommonWell record discovery and data location services, a Patient Record MUST be related to a Person Record.

CommonWell Person Identifier
This globally-unique identifier is created during Patient record creation and is associated with a CommonWell Person Record. An individual will be assigned, at most, one CommonWell Person Identifier. That is, an individual whose Visits and Patient Records have been back- loaded to CommonWell does not have an associated CommonWell Person Identifier or Person Record until that individual has been enrolled in CommonWell.

Patient Link
The relationship between a Person and Patient Record. Patient links are managed by the rules engine.

Network Link
The relationship between Patient records across organizational boundaries. Level of Link Assurance (LOLA) is the value expressing CommonWell's level of confidence in the network link. A network link must be LOLA 2 or higher to perform document query and retrieval.

Link ID
The MPI Link ID to which the patient record is linked.

Non-surviving Patient ID
The local Patient Identifier of the non-surviving Patient Record. The value is under the control of the local Edge

System and represents the unique identifier for the Patient Record in the local system.

5 Patient Identity Management

The document sharing model used by CommonWell requires that Edge Systems acting as document consumers resolve Patient Identity prior to querying documents. To facilitate Patient discovery and identity resolution, CommonWell provides a central service for Edge Systems to register Patient Identity and associated visit information to enable Patient discovery across the network of CommonWell Organizations.

5.1 Design Goals and Assumptions

The following are goals and assumptions for the CommonWell Patient Identity management service:

- CommonWell provides REST-based and PIX v2.x services for Patient Identity feed and query transaction processing.
- CommonWell will assign a globally unique Person Identifier linked to each registered patient. CommonWell will not provide the CommonWell Identifier to a document registry.
- The Edge System acting as a Patient Identity Source provides Patient Identity event notifications to both CommonWell PIX and the Edge System's document registry (which is known to CommonWell via the Edge System's Organization configuration).
- Edge Systems are NOT required to provide the CommonWell Identifier to a document registry.
- The process for communicating Patient Identity event notifications is outside the scope of this specification.
  The authoritative local Patient Identifier supplied by the Edge System to CommonWell MUST be the same as the one provided to the Edge System's document registry
- In terms of the IHE specifications, CommonWell represents a Patient Identifier Cross- reference Domain.
- CommonWell will NOT provide PIX update notifications. CommonWell does NOT represent an XDS Affinity Domain.

The CommonWell Identifier is not an XDS Affinity Domain Patient ID (XAD-PID). An XAD- PID is a Patient Identifier assigning authority which provides a single unique identifier for each patient for which documents are registered in the document registry. CommonWell does not represent an XDS Affinity Domain to the extent it is not providing document registration services and is not constrained by the XAD-PID Change Management (XPID) profile. The local Patient Identifier supplied to CommonWell by an Edge System may, in fact, be an XAD-PID. It remains the responsibility of the Edge System to ensure that any changes to the authoritative identifier for a patient in its Organization is communicated to CommonWell and that it remains synchronized with the Edge System's associated document registry.

6 Document Sharing

The CommonWell Health Alliance Broker (CHA Broker) provides centralized discovery and retrieval services capable of brokering transactions among a federated system of document registries and repositories.

6.1 Design Goals and Assumptions

The following are the goals and assumptions for the CommonWell document query and retrieval services.

- Edge Systems, acting as document consumers, do not need to contact each community that may hold documents for a targeted patient.
- The CHA Broker WILL support these IHE profiles: ITI-18, ITI-38, ITI-39 and ITI-43.
- The CHA Broker WILL support FHIR R4 Document Reference and Binary resources for FHIR-based document exchange.
- CommonWell Organizations MUST register their respective XCA/FHIR Responding Gateway services.
- CommonWell will NOT act as a document registry or repository.
- The CHA Broker will audit all transactions within the broker service itself ONLY. The CHA Broker will NOT act as an enterprise-wide audit repository.
- Edge Systems are responsible for auditing their own transactions.

7 API Security

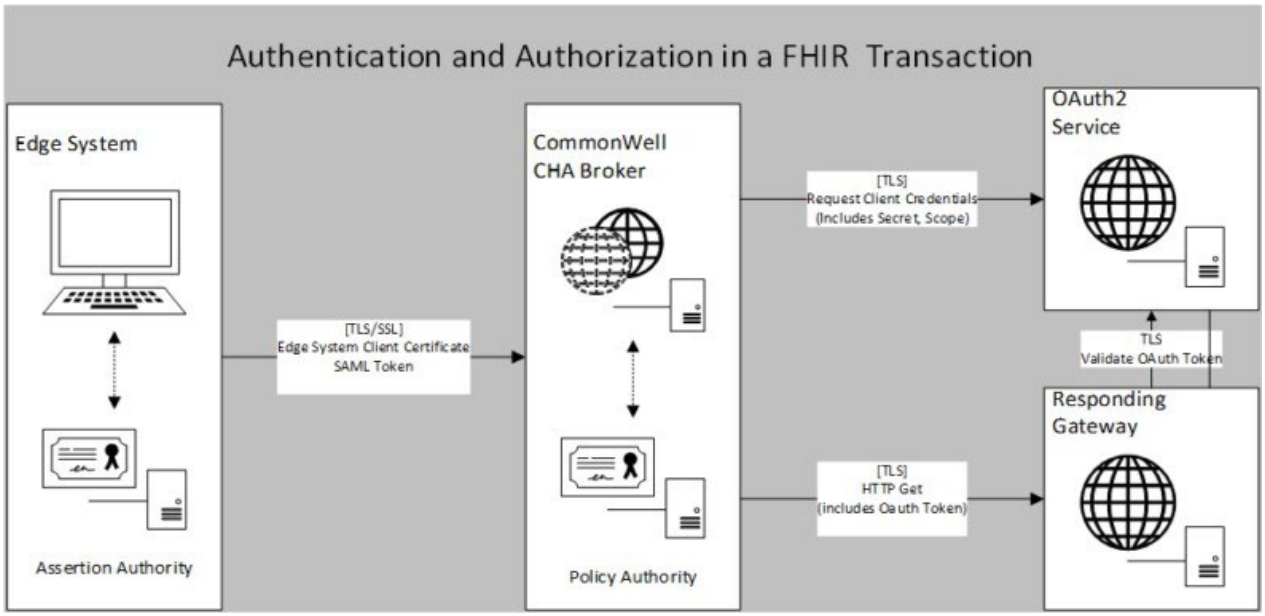
7.1 Transport Security

All message exchanges between CommonWell and Edge Systems MUST be secured using TLS.

7.1.1 X.509 Certificates for Authentication and Signing

X.509 Client Certificates are required for authentication of all transactions described in this specification (including authenticating to CommonWell REST APIs and the MLLP-based CommonWell Patient Identity Management service). In addition, SAML/JWT authorization tokens included in HTTP-based transactions must be signed using an X.509 Certificate.

Requests sent from an Edge System to CommonWell MUST use an X.509 Certificate maintained by the Edge System for authentication and for digitally signing the SAML/JWT authorization token included in the request. An Organization may use the same certificate for both authentication and signing, or a different certificate for each. The Organization provides the associated public key(s) to CommonWell as part of the Organization registration and configuration process in the CommonWell Management Portal.



Requests sent from CommonWell to an Organization's XCA Responding Gateway will include an X.509 Certificate maintained by CommonWell for client authentication. CommonWell will also sign SAML tokens presented to an Organization's XCA Responding Gateway using the same X.509 Certificate. CommonWell will provide the public key of this certificate to an Organization as part of the registration process.

7.1.2 OAuth2 for Authentication and Authorization of FHIR requests to Responding Gateways

Requests sent from CommonWell to an Organization's FHIR Responding Gateway will first get a token from an Organization's OAuth2 authorization server according to the Client Credentials Grant flow. This token will be presented to the Organization's FHIR Responding Gateway.

The OAuth2 server will be provided and maintained by the Organization. CommonWell's Management Portal will be used to configure the location, secret, and scopes for this OAuth server.

7.2 Certificate Requirements

All Client Certificates MUST meet or exceed the following criteria:

7.2.1 Key Sizes

- The CA shall utilize the SHA-256 algorithm for certificate signatures.
- All keys shall be at least 2048 bit (RSA).

7.2.2 Certificate Authority

The organization's certificate MUST be issued by a mutually trusted, WebTrust-certified Certificate Authority.

7.3 Federated Authentication

This section defines the exchange of metadata used to characterize the initiator of a request to the CommonWell server.

As a pre-condition to initiating a request to the CommonWell server, an Edge System MUST determine if a local user is authorized to perform a given function using the CommonWell services. If the request is authorized, the initiating Edge System attaches the user-centric assertions to the request. CommonWell receives the request with the understanding that the Edge System has locally authorized the user to make the request. An Edge System SHOULD audit all local authentication requests in accordance with ATNA.

For SOAP-based requests, the Edge System must convey the locally-authenticated user attributes and authorizations using SAML 2.0 assertions. The Edge System MUST issue, at minimum, one new token for each user session.

For REST-based requests, the Edge System will use a JSON Web Token (JWT). The Edge System MUST issue, at minimum, one new token for each user session.

For both SAML assertions and JSON Web Tokens, the expiration timestamp must be specified and digitally signed to prevent manipulation. The expiration timestamp MUST be set to no greater than eight (8) hours after generation to prevent reuse of the token. In SAML, the Expires element exists in the Timestamp element of the security header. In JWT, the expiration time is specified in the exp claim.

7.3.1 Claim Definitions

Security-related details are communicated to CommonWell services as claims included in either a JWT or SAML Assertion.

Standard Claims

Name	Type	Claim	Description
Subject ID	string	urn:oasis:names:tc:xspa:1.0:subject:subject-id	The name of the user as required by HIPAA Privacy Disclosure Accounting.
Subject Organization	string	urn:oasis:names:tc:xspa:1.0:subject:organization	In plain text, the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting.
Subject Role	code	urn:oasis:names:tc:xacml:2.0:subject:role	The SNOMED CT value representing the role that the user is playing when making the request.
Purpose of Use	code	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	The coded representation of the reason for the request.
Organization ID	string	urn:oasis:names:tc:xspa:1.0:subject:organization-id	A unique identifier for the organization that the user is representing in performing this transaction. The organization ID may be an Object Identifier (OID), or it may be a URL assigned to that organization.
National Provider Identifier	string	urn:oasis:names:tc:xspa:2.0:subject:npi	**Recommended**: A National Provider Identifier (NPI) is a unique 10-digit identification number issued to healthcare providers in the United States by the Centers for Medicare and Medicaid Services (CMS). Edge System should send NPI if known.
NAIC Source	string	http://commonwellalliance.org/claims/naicsource	Used in Payment and Operations use cases to assert who has the BAA relationship with the patient to access the PHI data. This value is provided by the Data Retrieval Service requestor and must contain the NAIC OID along with the NAIC Company Code. This is a required claim for all Operations and Payment purpose of use transactions. The value is validated against a maintained value set within the platform. **Sample Value** <AttributeValue>035678^^^urn:oid:2.16.840.1.113883.6.300</AttributeValue>
Audit Request Id	string	http://commonwellalliance.org/claims/auditrequestid	Used in Payment and Operations use cases to group all transactions for data retrieval requests pertaining to a single patient. This value is provided by the Data Retrieval Service requestor and must be the same for all workflow requests (patient discovery, document query, and retrieval) for a single patient.

			This is a required claim for all Operations and Payment purpose of use transactions. The value is validated against the cache of existing Audit Request Ids. **Sample Value** <AttributeValue>89c4d780-45d4-4109-b675-e78dd917e5c0</AttributeValue>
Home Community ID	string	urn:nhin:names:saml:homeCommunityId	The value shall be the Home Community ID (an Object Identifier) assigned to the Organization that is initiating the request, using the urn format (that is, "urn:oid:" appended with the OID). For information regarding OIDs, refer to http://www.oid-info.com/faq.htm. **Sample Value** <saml:Attribute Name="urn:nhin:names:saml:homeCommunityId"> <saml:AttributeValue>urn:oid:2.16.840.1.113883.3.190</saml:AttributeValue> </saml:Attribute>
Facility ID	string	http://commonwellalliance.org/claims/FacilityId	**OPTIONAL:** A unique identifier for the facility that the user is representing when performing the transaction. The facility will be an Object Identifier (OID). **NOTE:** This should only be used for organizations that are utilizing the facility model for managing organization hierarchies. If the facility ID is provided in the claims for the request, validation of the facility will be done during authentication. If the facility is invalid or inactive, the request will fail with a corresponding error message.
Facility Name	string	http://commonwellalliance.org/claims/FacilityName	**OPTIONAL:** In plain text, the name of the facility that the user is representing when performing the transaction. **NOTE:** This should be used for organizations that are utilizing the facility model for managing organizations.

JWT Claims

When using JWTs, the Edge System must also include the standard JWT-specific claims listed below.

Name	Type	Claim	Description
Audience	string	aud	The value for the audience claim must be *urn:commonwellalliance.org.*
Issuer	string	iss	The value for the Issuer claim must be *self*
Not Before	integer	nbf	The ”nbf” (not before) claim identifies the time before which the JWT MUST NOT be accepted for processing. The processing of the “nbf” claim requires that the current date/time MUST be after or equal to the not-before date/time listed in the “nbf” claim. Its value MUST be a number containing an IntDate value.
Expiration Time	integer	exp	The “exp” (expiration time) claim identifies the expiration time on or after which the JWT MUST NOT be accepted for processing. The processing of the “exp” claim requires that the current date/time MUST be before the expiration date/time listed in the “exp” claim. Its value MUST be a number containing an IntDate value (epoch datetime). The duration between the “exp” and the “nbf” claims cannot be more than eight (8) hours.

NOTE: The list of claims CommonWell provides when sending messages to Edge Systems is outside the scope of the CommonWell Services Specification. For an up-to-date list, refer to: Claims Values – Release of Information vs Treatment.

7.4 SAML in SOAP-based Transactions

SOAP-based service security is based on the NHIN Authorization Framework 3.0 (https://www.healthit.gov/sites/default/files/nhin-authorization-framework-production-specification- v3.0-1.pdf) (with exceptions noted below). When making SOAP-based requests to CommonWell, an Edge System MUST include the locally-authenticated user attributes and authorization claims described in section 7.3 Federated Authentication in the SAML token’s attribute statement.

When brokering SOAP-based requests to an Edge System’s responding gateway, CommonWell will package the claims submitted by the originating Edge System in the SAML token used in the request from CommonWell to the responding gateway identified by CommonWell as the destination for the brokered request. CommonWell will present a SAML token to the destination responding gateway using either a Bearer or Holder-of-Key subject confirmation; the subject confirmation method for the responding gateway is specified as part of the Organization registration process.

The implementation of the CommonWell SOAP-based services has additional constraints for use of SAML tokens:

- CommonWell currently supports the Bearer and Holder-of-Key subject confirmation methods for incoming SOAP requests.
- CommonWell DOES NOT support the Sender-Vouches subject confirmation method.
- For brokered requests sent from CommonWell to an Edge System responding gateway, the responding gateway MUST accept either the Bearer or Holder-of-Key subject confirmation method.

The following are examples of the Bearer and Holder of Key tokens:

Bearer Token Example

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
 <s:Header>
  <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RegistryStoredQuery</a:Action>
  <a:MessageID>urn:uuid:3965b675-51d9-40b8-aef6-8c400fdeeb6c</a:MessageID>
  <a:ReplyTo>
   <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
  </a:ReplyTo>
  <a:To
s:mustUnderstand="1">https://integration.chabroker.api.commonwellalliance.org/StoredQuery.svc</a:To>
  <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
   <u:Timestamp u:Id="_0">
    <u:Created>2016-08-24T15:28:20.266Z</u:Created>
    <u:Expires>2016-08-24T15:33:20.266Z</u:Expires>
   </u:Timestamp>
   <Assertion ID="_3f092082-0b05-44b6-9133-2cd08e5ce25b" IssueInstant="2016-08-24T15:28:20.250Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer>self</Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
     <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <Reference URI="#_3f092082-0b05-44b6-9133-2cd08e5ce25b">
       <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
       </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
       <DigestValue>enC6a/JhXXMHHIEFKI+gBuPehTWMuWDf0oHanVvJUiU=</DigestValue>
      </Reference>
     </SignedInfo>

<SignatureValue>Dj6Y3ti8+OJf7moYeF4xvjdTqyFsNQgu6ARSUJraNwvJrJp4iJZsXLX95cK8KNVifNxsw7JZqRh2X1
Ert6...</SignatureValue>
     <KeyInfo>
      <X509Data>

<X509Certificate>MIIF5TCCBM2gAwIBAgIJAOhxCyOqljX9MA0GCSqGSIb3DQEBCwUAMIHGMQswCQYDVQQG
Ew...</X509Certificate>
      </X509Data>
     </KeyInfo>
    </Signature>
    <Subject>
     <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
    </Subject>
    <Conditions NotBefore="2016-08-24T15:27:20.250Z" NotOnOrAfter="2016-08-24T16:58:20.250Z">
     <AudienceRestriction>
```

<Audience>urn:commonwellalliance.org</Audience>
</AudienceRestriction>
</Conditions>
<AttributeStatement>
<Attribute Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
<AttributeValue>John Doe</AttributeValue>
</Attribute>
<Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
<AttributeValue>Saint Andrews Medical Center</AttributeValue>
</Attribute>
<Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
<AttributeValue>2.16.840.1.113883.3.8.456.7897.1</AttributeValue>
</Attribute>
<Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
<AttributeValue>
<Role xsi:type="CE" code="CE" codeSystem="2.16.840.1.113883.6.96"
codeSystemName="SNOMED_CT" displayName="Pharmacist" xmlns="urn:hl7-org:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" />
</AttributeValue>
</Attribute>
<Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
<AttributeValue>
<PurposeOfUse xsi:type="CE" code="TREATMENT" codeSystem="2.16.840.1.113883.3.18.7.1"
codeSystemName="nhin-purpose" displayName="Treatment" xmlns="urn:hl7-org:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" />
</AttributeValue>
</Attribute>
</AttributeStatement>
</Assertion>
</o:Security>
</s:Header>
<s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<AdhocQueryRequest xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0">
<ResponseOption returnType="LeafClass" returnComposedObjects="true" />
<AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" xmlns="urn:oasis:names:tc:ebxml-
regrep:xsd:rim:3.0">
<Slot name="$XDSDocumentEntryPatientId">
<ValueList>
<Value>7819798^^^URN:OID:2.16.840.1.113883.3.8.456.7897.1</Value>
</ValueList>
</Slot>
<Slot name="$XDSDocumentEntryStatus">
<ValueList>
<Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')</Value>
</ValueList>
</Slot>
<Slot name="$XDSDocumentEntryType">
<ValueList>
<Value>('urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1','urn:uuid:34268e47-fdf5-41a6-ba33-
82133c465248')</Value>
</ValueList>

```
      </Slot>
    </AdhocQuery>
   </AdhocQueryRequest>
  </s:Body>
</s:Envelope>
```

Holder of Key Token Example

```
<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
	<soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
		<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
			<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="a4f3464a-7dd4-41f7-907b-b0cb5dbb3fb7"
IssueInstant="2016-07-19T13:22:34Z" Version="2.0">
				<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:X509SubjectName">CN = GeoTrust DV SSL CA - G3, OU = Domain Validated SSL, O = GeoTrust Inc., C =
US</saml2:Issuer>
				<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
					<SignedInfo>
						<CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
						<SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
						<Reference URI="#a4f3464a-7dd4-41f7-907b-b0cb5dbb3fb7">
							<Transforms>
								<Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
								<Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
							</Transforms>
							<DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

	<DigestValue>/F4X2QjBNlZ93sIbQtWMyMvt0r4=</DigestValue>
						</Reference>
					</SignedInfo>

	<SignatureValue>auoc4jmzjMHqTGD8/8MwMvpus3ssYF7HgtFOGVQAXCaINQ/hwxZhdaNUcApjqvWSj
7FU2Reim5Wy
SP05hXiXDKd8brAm/lUCAgOG9ygFfff2Ed4cbBQOJESXmoYi6afau0YMCIKlC21ebCaZBwYImRY9
jggd/W74PsfDMKdgiMQraHwo8WxuvF5z1...</SignatureValue>
					<KeyInfo>
						<X509Data>

	<X509Certificate>MIIF6DCCBNCgAwIBAgIQGwE2jlspNVoOpo7hwdAIozANBgkqhkiG9w0BAQsFADBm
MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjEdMBsGA1UECxMURG9tYWluIFZhbGlkYXRlZCBT
U0wxIDAeBgNVBAMTF0dlb1RydXN0IERWIFNTTCBDQSAtIEczMB4XDTE2MDYwODAwMDAwMFoXDTE3
MDYwODIzNTk1OVowNDEyMDAGA1UEAwwpaGl...</X509Certificate>
						</X509Data>
					</KeyInfo>
				</Signature>
				<saml2:Subject>
					<saml2:SubjectConfirmation
```

```
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
                        </saml2:Subject>
                        <saml2:Conditions NotBefore="2016-07-19T12:22:34Z" NotOnOrAfter="2016-
07-19T14:22:34Z">
                                <saml2:AudienceRestriction>

        <saml2:Audience>urn:commonwellalliance.org</saml2:Audience>
                                </saml2:AudienceRestriction>
                        </saml2:Conditions>
                        <saml2:AuthnStatement AuthnInstant="2016-07-19T13:22:34Z">
                                <saml2:SubjectLocality Address="localhost" DNSName="ShinnyClient"
/>
                                <saml2:AuthnContext>

        <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml2:AuthnContext
ClassRef>
                                </saml2:AuthnContext>
                        </saml2:AuthnStatement>
                        <saml2:AttributeStatement>
                                <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-
id">
                                        <saml2:AttributeValue>John Doe</saml2:AttributeValue>
                                </saml2:Attribute>
                                <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
                                        <saml2:AttributeValue>Saint Andrews Medical
Center</saml2:AttributeValue>
                                </saml2:Attribute>
                                <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">

        <saml2:AttributeValue>2.16.840.1.113883.3.8.456.7897.1</saml2:AttributeValue>
                                </saml2:Attribute>
                                <saml2:Attribute Name="urn:nhin:names:saml:homeCommunityId">

        <saml2:AttributeValue>urn:oid:2.16.840.1.113883.3.8.456.7897.1</saml2:AttributeValue>
                                </saml2:Attribute>
                                <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
                                        <saml2:AttributeValue>
                                                <Role xmlns="urn:hl7-org:v3" code="112247003"
codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName="Medical doctor"
xsi:type="CE" />
                                        </saml2:AttributeValue>
                                </saml2:Attribute>
                                <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
                                        <saml2:AttributeValue>
                                                <PurposeOfUse xmlns="urn:hl7-org:v3"
code="TREATMENT" codeSystem="2.16.840.1.113883.18.7.1" codeSystemName="nhin-purpose"
displayName="Treatment" type="CE" />
                                        </saml2:AttributeValue>
                                </saml2:Attribute>
                        </saml2:AttributeStatement>
```



```
                </saml2:Assertion>
            </wsse:Security>
            <wsa:To
soapenv:mustUnderstand="true">https://integration.chabroker.api.commonwellalliance.org/StoredQuery.svc
</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:2139562c-2134-3c1e-cf6c-
00155d004f8f</wsa:MessageID>
            <wsa:Action
soapenv:mustUnderstand="true">urn:ihe:iti:2007:RegistryStoredQuery</wsa:Action>
        </soapenv:Header>
        <soapenv:Body>
            <query:AdhocQueryRequest xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
                <query:ResponseOption returnComposedObjects="true" returnType="LeafClass" />
                <rim:AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
                    <rim:Slot name="$XDSDocumentEntryPatientId">
                        <rim:ValueList>

        <rim:Value>'7819798^^^&amp;amp;2.16.840.1.113883.3.8.456.7897.1&amp;amp;ISO'</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryStatus">
                        <rim:ValueList>
                            <rim:Value>('urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved')</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryCreationTimeFrom">
                        <rim:ValueList>
                            <rim:Value>20110721</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryCreationTimeTo">
                        <rim:ValueList>
                            <rim:Value>20160720</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryType">
                        <rim:ValueList>
                            <rim:Value>('urn:uuid:7edca82f-054d-47f2-a032-
9b2a5b5186c1','urn:uuid:34268e47-fdf5-41a6-ba33-82133c465248')</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                </rim:AdhocQuery>
            </query:AdhocQueryRequest>
        </soapenv:Body>
</soapenv:Envelope>
```

7.5 JSON Web Token (JWT) for REST-based services

When making REST-based requests to the CommonWell server, an Edge System MUST include authorization claims in the form of a JWT bearer token in the *Authorization* HTTP Header of the request.

JSON Web Token (http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-08) (JWT) is a compact URL-safe means of representing and transferring claims from an Edge System to the CommonWell server. The claims in a JWT are encoded as a JavaScript Object Notation (JSON) object and added to the payload of a JSON Web Signature (JWS) structure. The JWT is digitally signed and encrypted. Below is an example of a request with a message authentication code (MAC) encrypted, base64url encoded JWT token in the HTTP *Authorization* header.

The following is an example of the payload of the JWT token. Note that the names of the claims observe the same convention described in the NHIN authorization framework.

Example of Payload of JWT Token

```
{
 "iss": "self",
 "aud": "urn:commonwellalliance.org",
 "nbf": 1380560162,
 "exp": 1380560455,
 "urn:oasis:names:tc:xacml:2.0:subject:role": "112247003",
 "urn:oasis:names:tc:xspa:1.0:subject:subject-id": "Geoffrey Geiger",
 "urn:oasis:names:tc:xspa:1.0:subject:organization": "St. Barnabas Hospital",
 "urn:oasis:names:tc:xspa:1.0:subject:organization-id": "2.16.840.1.113883.4",
 "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse": "TREATMENT",
 "urn:oasis:names:tc:xspa:2.0:subject:npi": "1770589525"
}
```

The following example shows the encoded JWT inserted as a bearer token in the HTTP Authorization header.

Sample Request JWT Web Token

```
GET https://rest.api.commonwellalliance.org/v1/person/c21cc31d-6c57-442b-8e76-5de498903334 HTTP/1.1
Host: rest.api.commonwellalliance.org
Authorization: Bearer eyJhbGciOiJSU0.WnDYvpIAeZ72deHxz3roJDXQyhxx0wKaM.fiK51VwhsxJ-siBMR-YFiA
```

7.6 Delegation of Authority

Before an organization can send delegated requests, several prerequisites must be met:

- **Delegation of Authority can be used for any of these network**
  - **CommonWell**
  - **Carequality**
    - **Publication to CeQ Directory:** Any organization designated as a delegate for any member must be published to CeQ Directory with the name as DelegateOID-OBO-PrincipalOID
  - **TEFCA**
    - **Publication to TEFCA RCE Directory**: Any organization designated as a delegate for any member must be published in the TEFCA Recognized Coordinating Entity (RCE) directory. This ensures that the delegate is recognized and authorized within the TEFCA framework.
- **Principal Enablement**:

    - For CommonWell and CareQuality
        - The member organization must enable them as Principal under the Network tab of the Organization Portal. This step is crucial for establishing the member's authority to delegate.
    - For TEFCA
        - The member organization must enable them as Principals under the TEFCA tab of the Organization Portal. This step is crucial for establishing the member's authority to delegate.
- **Delegate Addition**: The member must add the delegate organization through the Include/Exclude/DoA (Delegation of Authority) tab in the Organization Portal. This formalizes the delegation relationship within the system.
- **Configuration Publication**: Sufficient time must pass after the member has added the delegate to ensure that the Delegation of Authority configurations are published to the RCE directory. This delay allows for the proper propagation and validation of the delegation settings.

When sending delegated requests, the delegate organization must include information about the principal organization.

Steps for communication over IHE

- The element **MUST** have the `FriendlyName` set to "QueryAuthGrantor".
- The value **MUST** be the Directory Entry assigned to the Principal for whom the Delegate is initiating the request, formatted using the FHIR (Fast Healthcare Interoperability Resources) Resource format.

This ensures that all delegated requests are properly authenticated and traceable to the principal organization, maintaining the integrity and security of the TEFCA network.

Example:

```
<saml:Attribute FriendlyName=”QueryAuthGrantor”>
<saml:AttributeValue>Organization/2.16.840.1.113883.3.7204.1</saml:Attribute
Value>
</saml:Attribute>
```

Steps for communication over FHIR

Please note, when a delegate intends to call FHIR endpoints, it is essential that the information regarding Delegation of Authority, which is present in the SAML, is also included in the JWT token.
Example:

For CommonWell and CareQuality

```
"QueryAuthGrantor": "Organization/urn:oid:2.16.840.1.113883.3.7204.1"
```

For TEFCA, the value must be passed inside the "tefca_dra" extension

```
“extensions”:{

     “tefca_dra”: {

          “queryAuthGrantor”:
“Organization/urn:oid:2.16.840.1.113883.3.7204.1”
```

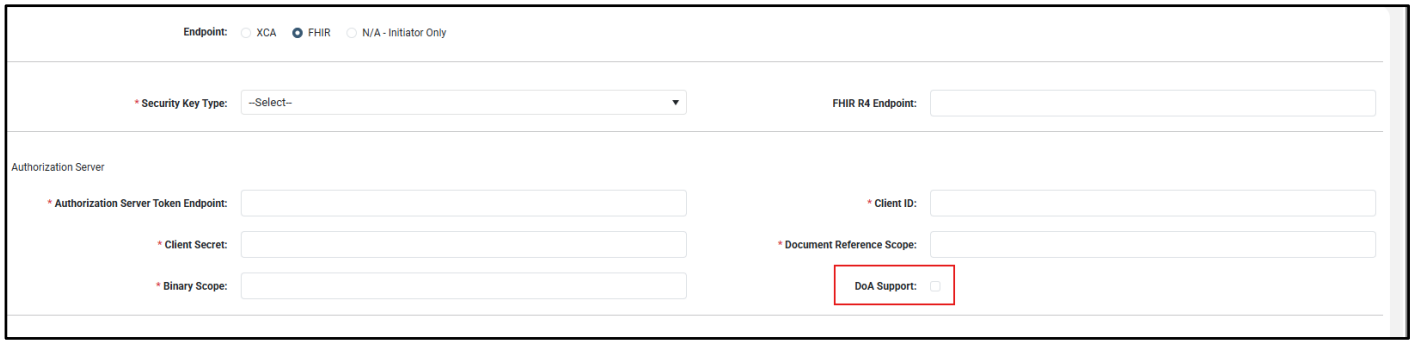


```
        }

}
```

Prerequisites for the responding organizations (FHIR)

- As the token can only be generated by the auth server, the responding organizations must support embedding the QueryAuthGrantor value in the token. Once they do so, they must declare their support in the Portal



- After you declare the DoA Support, CommonWell broker will pass the value of "QueryAuthGrantor" while calling the token endpoint, and will expect the token to include that claim

8 REST API

CommonWell provides REST services that support workflows facilitating Patient Management (Section 8.3) and Patient Identification and Linking (Section 8.4).

8.1 Service Root URL

The Service Root URL is the address where all of the resources defined by this interface are found.

- Integration: https://api.integration.commonwellalliance.lkopera.com/
- Production: https://api.commonwellalliance.lkopera.com

8.2 Resources

8.2.1 Error

A read-only representation of error information.

Error Example


```
{
        "message": "Patient consent policy forbids access to this resource.",
        "code": 1245,
        "reference": "f57236f0-d4ad-11e2-8b8b-0800200c9a66",
        "help": {"href": "http://rest.api.commonwellalliance.org/help/#consent"}
}
```


8.2.2 Organization

Based on the FHIR formal definition of an Organization resource

(http://www.hl7.org/implement/standards/fhir/organization-definitions.htm), a CommonWell Organization represents an institution, corporation, department, community group, practice group, or other organization participating as an initiator or responder in the workflows supported by the CommonWell services.

CommonWell organizations, as identified by their Organization ID (OID), MUST be unique within the network. To ensure unique identifiers system-wide and reduce potential conflicts among Service Adopters and organizations, CommonWell requires provisioning an OID from HL7 (https://www.hl7.org/oid/) or Internet Assigned Numbers Authority (IANA)
(https://www.iana.org/).

Organization Example


```
{
        "organizationId": "2.16.840.1.113883.3.9960.25.1.2",
        "homeCommunityId": "2.16.840.1.113883.3.9960.25.1.2",
        "name": "St. Barnabas Hospital",
        "displayName": "St. Barnabas Hospital",
        "memberName": "CW Service Adopter 1",
```

```
"type": "Acute Care",
"patientIdAssignAuthority": "2.16.840.1.113883.3.9960.25.1.2",
"alternatePatientIdAssignAuthority": [
        {
                "system": "1.20.4.18.35.2.60.12.64.3.1.72713.1",
                "assigner": "TransUnion",
                "purpose": "ID Proof Vendor",
        },
],
"securityTokenKeyType": "Bearer",
"sendingFacility": {
        "namespaceId": "string",
        "universalId": "string",
        "universalIdType": "string"
},
"sendingApplication": {
        "namespaceId": "string",
        "universalId": "string",
        "universalIdType": "string"
},
"isActive": true,
"locations": [
        {
                "address1": "8123 Hawthorne Ave",
                "address2": "",
                "city": "Chicago",
                "state": "IL",
                "postalCode": "60612",
                "country": "USA",
                "phone": "708-555-1234",
                "fax": "708-555-2345",
                "email": "sbh@example.com"
        }
],
"technicalContacts": [
        {
                "name": "Jane Doe",
                "title": "Technical Support",
                "email": "jdoe@example.com",
                "phone": "708-555-3456"
        }
],
"gateways": [
        {
                "serviceType": "R4_Base",
                "gatewayType": "FHIR",
                "endpointLocation": "https://fhir.sbh.example.com",
        }
],
"authorizationInformation": {
        "authorizationServerEndpoint": "string",
        "clientId": "string",
        "clientSecret": "string",
```



```
                "documentReferenceScope": "string",
                "binaryScope": "string"
        },
        "networks": [
                {
                        "type": "CommonWell",
                        "purposeOfUse": [
                                {
                                        "id":  "TREATMENT",
                                        "queryIniatorOnly": "false",
                                        "queryInitiator": "true",
                                        "queryResponder": "true",
                                }
                        ]
                        "includes": [
                                "2.16.840.1.113883.3.9960.25.1.3","2.16.840.1.113883.3.9960.25.1.4"
                        ],
                        "excludes": [
                                "2.16.840.1.113883.3.9960.25.1.5"
                        ],
                }
        ]
}
```


Link Relations

An Organization resource may contain the reserved *_links* property, a collection of links available to the Edge System against this Organization resource given its current state.

Link	Description
self	Reference to this organization representation.

8.2.3 Secondary or Alternate ID

The Patient object supports Secondary or Alternate ID. These identifiers are non-local identifiers, e.g. driver's license number, may be used as part of the autolinking workflow.

An alternate ID provided by a third-party identity proofing service is required for the CommonWell Organization to participate in the CommonWell Patient Access Data request use case.

A secondary or alternate ID may be added to the patient object in the following ways:

1. REST API: Create and Update Patient, where identifier.use = "secondary".
2. PIX: Additional identifiers may be added to the PID-3 Patient Identifier List.
    a. Example: 6676^^^&12.8.2014&ISO~12290^^^&1.2.3.4.5&ISO

The Secondary or Alternate Assigning Authority responsible for issuing the alternate ID may be registered to that Organization within the Management Portal.

Patient attributes specifically associated with the alternate ID may be added to the alternatePatients field in the Patient object.

8.3 Patient Management

8.3.1 Create and Update Patient

This endpoint is used to Create or Update a Patient's demographics in the MPI using the local patient identifier. The system automatically checks to see if a Patient exists based on the Patient ID, Org ID, and Assigning Authority provided.

- If the Patient exists, then the record will update.
- If no match is found, then a new Patient will be created.

Assigning Authority must be associated with the Org ID.

If there is a mismatch between Org ID and Assigning Authority for an existing patient record, then the request response will return an error, and the patient record will not be updated.

POST /v2/org/{OrgId}/Patient	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • **Example: /v2/org/2.16.840.1.113884.3.101/Patient**
Request Body	Patient Object. See 8.4.6 Patient Object. Note: Assigning Authority required in the request body.
Response	Returns PatientCollection object with a "Self" link to the patient record that was created. Note the Patient object is not returned here.

8.3.2 Get Patient

An Edge System can retrieve Patient record from MPI based on the local patient identifier.

GET **/v2/org/{OrgId}/Patient/{PatientID}**	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue*^^^&*PatientIdAssignAuthority*& *PatientIdAssignAuthorityType* **Example: /v2/org/2.16.840.1.113884.3.101/Patient/10000%5E%5E%5E%262.16.840.1.113884.3.101.1%26ISO**

Request Body	None
Response	Returns Patient Object based on the local patient identifier along with Link collection associated with the patient. Links are provided only for patients associated with the Organization identified in the calling context.

Example Response:


```
{
    "Patients": [
        {
            "Links": {
                "Self":
"https://api.integration.commonwellalliance.lkopera.com/v2/org/2.16.840.1.113883.3.2611.9.99.101/Patient/601%5e%5e%5e%262.16.840.1.113883.3.2611.9.99.101.1%26ISO",
                "PatientLink":
"https://api.integration.commonwellalliance.lkopera.com/v2/org/2.16.840.1.113883.3.2611.9.99.101/PatientLink/601%5e%5e%5e%262.16.840.1.113883.3.2611.9.99.101.1%26ISO",
                "ResetLink":
"https://api.integration.commonwellalliance.lkopera.com/v2/org/2.16.840.1.113883.3.2611.9.99.101/Patient/601%5e%5e%5e%262.16.840.1.113883.3.2611.9.99.101.1%26ISO/ResetLink",
                "Delete":
"https://api.integration.commonwellalliance.lkopera.com/v2/org/2.16.840.1.113883.3.2611.9.99.101/Patient/601%5e%5e%5e%262.16.840.1.113883.3.2611.9.99.101.1%26ISO",
                "ProbableLink":
"https://api.integration.commonwellalliance.lkopera.com/v2/org/2.16.840.1.113883.3.2611.9.99.101/ProbableLink/601%5e%5e%5e%262.16.840.1.113883.3.2611.9.99.101.1%26ISO"
            },
            "Patient": {
                "identifier": [
                    {
                        "value": "601",
                        "period": {
                            "start": "2010-09-12"
                        },
                        "system": "2.16.840.1.113883.3.2611.9.99.101.1",
                        "use": "official"
                    },
                    {
                        "value": "95D0E3A9-2977-499F-9AAD-699EBA853427",
                        "system": "2.16.840.1.113883.3.9960.1.35.99.40",
                        "use": "official"
                    }
                ],
                "address": [
                    {
                        "line": [
                            "511 Main St"
                        ],
```



```
                "city": "Kingston",
                "state": "NY",
                "postalCode": "12401",
                "use": "home",
                "type": "both",
                "period": {
                    "start": "2010-09-12"
                }
            }
        ],
        "birthDate": "1969-10-24",
        "gender": "M",
        "name": [
            {
                "family": [
                    "Anderson"
                ],
                "given": [
                    "David"
                ],
                "text": "David Anderson",
                "prefix": [
                    "Mr"
                ],
                "suffix": [],
                "use": "usual",
                "period": {
                    "start": "2010-09-12"
                }
            }
        ],
        "telecom": [
            {
                "system": "phone",
                "use": "home",
                "value": "(222) 222 2228",
                "period": {
                    "start": "2010-09-12"
                }
            }
        ],
        "active": true,
        "managingOrganization": {
            "identifier": [
                {
                    "system": "2.16.840.1.113883.3.2611.9.99.101"
                }
            ],
            "name": "ELLKAY Test Account 01"
        }
```



```
            }
        }
    ],
    "status": {
        "message": "Patients successfully retrieved.",
        "code": 200
    }
}
```


8.3.3 Delete Patient

This endpoint will delete a Patient in MPI. Once deleted, the patient will no longer be available, and future GET requests will return a 404 Not Found. Edge Systems can only delete local patients associated with their organization.

DELETE /v2/org/{OrgId}/Patient/{PatientID}	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue*^^^&*PatientIdAssignAuthority*&*PatientIdAssignAuthorityType* **Example:** **/v2/org/2.16.840.1.113884.3.101/Patient/10000%5E%5E%5E%262.16.840.1.113884.3.101.1%26ISO**
Request Body	None
Response	Returns Response Status Object with error codes if any.

8.3.4 Merge Patient

When two patients are merged, an Edge System can send a request to merge both patients.
The Patient ID of the active patient record and the Patient ID of non-surviving Patient record is required for the merge process. The URL contains the non-surviving Patient ID while the request body contains the surviving Patient ID.

Demographics data of the non-surviving patient will become the historical demographics data for the surviving (Active) patient.

PUT **/v2/org/{OrgId}/Patient/{NonSurvivingPatientID/Merge**

<table>
<tr><td>Parameters</td><td>

OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System.
NonSurvivingPatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type
format: IdentifierValue^^^&PatientIdAssignAuthority&PatientIdAssignAuthorityType

Example:
/v2/org/2.16.840.1.113884.3.101/Patient/10000%5E%5E%5E%262.16.840.1.113884.3.101.1%26ISO/Merge
</td></tr>
<tr><td>Request Body</td><td>
The merge request body should contain a link to the surviving patient.

link.other.reference = Patient ID of the surviving patient formatted as “Patient/{survivingPatientId}^^^&{survivingPatientAssigningAuthorityId}&{survivingPatientAssigningAuthorityIdType}”

link.type should be “replaced-by” – for Merge Patients; the link refers to the Active Patient. The patient resource containing this link is the non-surviving patient.

In the example below:

Non-surviving Patient ID is 10000 (Included in the Request parameter)

surviving Patient ID is 10150 (Included in the Request body)

<code>PUT /v2/org/2.16.840.1.113884.3.101/Patient/10000%5E%5E%5E%262.16.840.1.113884.3.101.1%26ISO/Merge</code>

<pre>
{
    "link": {
        "other": {
            "reference":
"Patient/10150^^^&2.16.840.1.113884.3.101.1&ISO/"
        },
        "type": "replaced-by"
    }
}
</pre>
</td></tr>
<tr><td>Response</td><td>Returns Status Object with error codes if any.</td></tr>
</table>

8.3.5 Patient Disclosure

An Edge System can set the disclosure flag for patient. This will determine if the patient’s data should be shared with other organizations.

By default, patients will inherit the purpose of use (POU) settings based on their organization's settings in the Admin Portal. Patients can opt out of participating in one of the POU. The Edge System or a Patient portal can call this endpoint to update the POU settings in MPI.

POST **/v2/org/{OrgId}/Patient/{PatientID}/Disclosure**	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue*^^^&*PatientIdAssignAuthority*&*PatientIdAssignAuthorityType*

Request Body	{
	"consentToDisclose": true,
	"disclosure": [
	{
	"networks": [
	{
	"code": "CommonWell",
	"purposeOfUse": [
	{
	"code": "TREATMENT",
	"consent": true
	},
	{
	"code": "REQUEST",
	"consent": true
	},
	{
	“code”: “Carequality”,
	“purposeOfUse”: [
	{
	“code”: “TREATMENT”,
	“consent”: true
	},
	{
	“code”: “REQUEST”,
	“consent”: true
	},
	{
	“code”: “PAYMENT”,
	“consent”:
	false
	}
	]
	}
	]
	}

```
        ]
    }
}
```
 |
| **Response** | Returns ResponseStatus Object with error codes if any. |

GET /v2/org/{OrgId}/Patient/{PatientID}/Disclosure	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue^^^&PatientIdAssignAuthority&PatientIdAssignAuthorityType*
Response
```
{
        "consentToDisclose": true,
        "disclosure": [
            {
                "networks": [
                    {
                        "code": "CommonWell",
                        "purposeOfUse": [
                            {
                                "code": "TREATMENT",
                                "consent": true
                            },
                            {
                                "code": "REQUEST",
                                "consent": true
                             },
                    {
                           “code”:  “Carequality”,
                           “purposeOfUse”:  [
                            {
                                  “code”: “TREATMENT”,
                                  “consent”: true
                            },
                            {
                                   “code”: “REQUEST”,
                                   “consent”: true
                            },
                            {
                                   “code”: “PAYMENT”,
                                   “consent”:
false                             }
                        ]
```
 |

8.3.6 Event Notification Services

Event Notification Services (ENS) allow Members to enable patient alerts for their Organizations to receive notifications when an existing patient link is updated. Published events will be transmitted in the v2 Patient Collection JSON format. This enables members to be notified of demographic changes and view the updated patient link the same way they would if they performed a Get Patient Link request.

Configuration

Member admins can configure settings for ENS via the management portal with options to subscribe themselves and their organizations to receive notifications at the member-level endpoint that they provide. They are also able to set whether their organizations can opt-out of the subscription or provide their own endpoint. Based on the settings configured for their organizations by the member admin, organization specific ENS settings can also be configured at the Organization settings level.

To receive notifications, the Member and/or the Organization must provide an HTTPS endpoint where notifications can be sent. This is done by exposing an endpoint that can handle HTTP POST requests. The Member can configure or update the organization's endpoint via the management portal. The Member and/or Organization must also load and trust the ELLKAY Client Certificate for the provided ENS endpoint. The certifications are available on the CommonWell Member SharePoint in the Certifications for ENS folder.

Authentication and Response

For security, calls to the configured HTTP endpoint will be authenticated by the service provider using an mTLS client certificate that gets sent to the subscribed Organization.
The payload that is received in response would be identical to the Get Patient Links payload.

Response

```
{
   "Patients": [
      {
         "Links": {
            "Self":
"v2/org/1.2.840.113549.1.1/Patient/704%5e%5e%5e%261.2.840.113549.1.1.1%26ISO",
            "Unlink":
"v2/org/1.2.840.113549.1.1/Patient/704%5e%5e%5e%261.2.840.113549.1.1.1%26ISO/patientLink
/D9500583-6755-492A-9C35-0D396B7501ED/Unlink"
         },
         "Patient": {} // Refer to Patient Object
      }
   ]
}
```

8.4 Patient Identification and Linking

A link is an association between Patient records or between Patient record and Person. There are two ways to create links:

1. System link or autolinking – This link type is done automatically by the Rules Engine and links Patient(s) to Person.
2. Manual link – This link type is done by an Edge System to associate patient records from a list of probable matches. The manual link workflow is available for Treatment exchange only and cannot be used for patient Request/IAS.

Level of Link Assurance (LOLA) is a value expressing CommonWell's level of confidence in a Network link (the relationship between Patient records across Organizational boundaries). Each level is defined as the following:

- LOLA 1: Established by CommonWell's probabilistic matching algorithm, LOLA 1 identifies a presumptive match between a local Patient Record and a remote Patient Record. LOLA 1 links are returned in the Get Probable Links endpoint and kicks off the manual link workflow. These links cannot be used for document query and retrieval.
- LOLA 2: Identifies a network relationship between Patient Records that are confirmed patient links that have either been established via autolinking or manual linking. These links are returned in the Get Patient Links endpoint.
- LOLA 3 (not implemented): Identifies a network relationship between Patient Records that has been validated using demographic information and an authoritative ID.
- LOLA 4 (not implemented): Identifies a network relationship between Patient Records that has been validated using biometric data.

The LOLA values are automatically managed by the system.

A network link MUST be LOLA 2 or higher for document query and retrieval.

For more information about CommonWell MPI 2.0 and Patient Matching, refer to the linked articles on the CommonWell Member SharePoint.

When a Demographics request includes a multi-part given name, the MPI returns matches for records with the full multi-part name and records with only the first token of the given name (e.g., 'Mary Ann' matches 'Mary Ann' and 'Mary')

8.4.1 Get Patient Links

An Edge System can search and request Patient Links by a local patient identifier. The result of the query will include local and remote patient's links that are autolinked by the rules engine or manually linked.

The links returned are confirmed links of LOLA 2 or higher.

GET **/v2/org/{OrgId}/PatientLink/{PatientID}**

GET
/v2/org/{OrgId}/PatientLink?fname={fname}&lname={lname}&dob={dob}&gender={gender}&zip={zip}

<table>
<tr><td>Parameters</td><td>

OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System.
PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type
Format: IdentifierValue^^^&PatientIdAssignAuthority& PatientIdAssignAuthorityType

OR

OrgId = Unique Organization OID
fname = Patient’s First Name or Patient’s First Name and Middle Name
lname = Patient’s Last Name or Patient’s Last Name and Middle Name
dob = Patient’s Date of Birth in yyyy-mm-dd format
gender = Patient’s Gender

Possible values: M (Male); F (Female); U (Unknown); O (Other)

zip = Patient’s ZIP code
***Fname, Lname, DOB and zip are required parameters to get links for a specific patient.

</td></tr>
<tr><td>Request Body</td><td>None</td></tr>
<tr><td>Response</td><td>
<pre>
{
    "Patients": [
        {
            "Links": {
                "Self":
"v2/org/1.2.840.113549.1.1/Patient/704%5e%5e%5e%261.2.840.113549.1.1.1%26ISO"
,
                "Unlink":
"v2/org/1.2.840.113549.1.1/Patient/704%5e%5e%5e%261.2.840.113549.1.1.1%26ISO/
patientLink/D9500583-6755-492A-9C35-0D396B7501ED/Unlink"
            },
            "Patient": {} // Refer to Patient Object
        }
    ]
}
</pre>
</td></tr>
</table>

8.4.2 Get Probable Links

An Edge System can request probable patient links by a local patient identifier. MPI will identify probable patients based on MPI match scores that are within a certain threshold range but are not auto matched.

Probable matches are determined by probabilistic algorithms. This will enable Edge Systems to confirm additional patient matches across other organizations. On confirmation, the patient will be matched to a person. Probable links need to be manually linked to the local patient before documents can be requested.

The links returned are LOLA 1.

GET **/v2/org/{OrgId}/ProbableLink/{PatientID}**

GET
/v2/org/{OrgId}/ProbableLink?fname={fname}&lname={lname}&dob={dob}&gender={gender}&zip={zip}

Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue^^^&PatientIdAssignAuthority& PatientIdAssignAuthorityType* OR • OrgId = Unique Organization OID • fname = Patient's First Name or Patient's First Name and Middle Name • lname = Patient's Last Name or Patient's First Name and Middle Name • dob = Patient's Date of Birth in yyyy-mm-dd format • gender = Patient's Gender ○ Possible values: M (Male); F (Female); U (Unknown); O (Other) • zip = Patient's ZIP code ***Fname, Lname, DOB, and zip are required parameters when getting links for the specific patient.
Request Body	None

Response	{
	"Patients": [
	{
	"Links": {
	"Self": "v2/org/1.2.840.113549.1.2/Patient/413%5e%5e%5e%261.2.840.113549.1.1.2%26ISO",
	"Link": "v2/org/1.2.840.113549.1.2/Patient/413%5e%5e%5e%261.2.840.113549.1.1.2%26ISO/PatientLink/001B590E-B2CD-4ADC-B654-8C8990941F77/Link",
	"Unlink": "v2/org/1.2.840.113549.1.2/Patient/413%5e%5e%5e%261.2.840.113549.1.1.2%26ISO/PatientLink/001B590E-B2CD-4ADC-B654-8C8990941F77/Unlink"
	},
	"Patient": {} // Refer to Patient Object
	}
	]
	}

8.4.3 Link Patient

An Edge System reviews the probable matches. An Edge System can link remote patient(s) if these patients are the same as local patient.

Use the response from Get Probable Links to find the LinkID.

Remote patients will be linked with the local patient and now considered as a manual confirmed LOLA 2 link.

PUT **/v2/org/{OrgId}/Patient/{PatientID}/PatientLink/{LinkID}/Link**	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue*^^^&*PatientIdAssignAuthority*& *PatientIdAssignAuthorityType* • LinkID- MPI Link ID Example: "v2/org/1.2.840.113549.1.2/Patient/413%5e%5e%5e%261.2.840.113549.1.1.2%26ISO/patientLink/001B590E-B2CD-4ADC-B654-8C8990941F77/Link"
Request Body	None
Response	Returns ResponseStatus Object with error codes if any.

8.4.4 Unlink Patient

After reviewing remote patient links for their local patient, an Edge System can unlink a remote patient that does not belong in the Patient collection and remove the existing LOLA2 network link.

Use Get Patient Links to find the LinkID.

Patient Links that are manually unlinked will no longer be autolinked to the same patient in the future by the matching algorithm.

PUT **/v2/org/{OrgId}/Patient/{PatientID}/PatientLink/{LinkID}/Unlink**	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System.

	• PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue^^^&PatientIdAssignAuthority& PatientIdAssignAuthorityType* • LinkID- MPI Link ID **Example:** "v2/org/1.2.840.113549.1.2/Patient/413%5e%5e%5e%261.2.840.113549.1.1.2%26ISO/patientLink/001B590E-B2CD-4ADC-B654-8C8990941F77/Unlink"
Request Body	None
Response	Returns ResponseStatus Object with error codes if any.

8.4.5 Reset Patient Links

Edge Systems can perform a "reset" to a Patient which will detach all LOLA 2 links to the specified Patient. This patient may be linked to the same collection of Patients (Person) again in the future.

Use Get Patient Links to find the LinkID.

PUT **/v2/org/{OrgId}/Patient/{PatientID}/ResetLink**	
Parameters	• OrgId – Identifies the Patient Identity Domain owned by the Organization represented by the Edge System. • PatientID – The local Patient Identifier. The value is under the control of the local Edge System and represents the unique identifier for the Patient Record in the local system. The format for this identifier MUST follow the HL7 CX data type format: *IdentifierValue^^^&PatientIdAssignAuthority& PatientIdAssignAuthorityType* • **Example:** "v2/org/1.2.840.113549.1.2/Patient/413%5e%5e%5e%261.2.840.113549.1.1.2%26ISO/ResetLink"
Request Body	None
Response	Returns Status Object with error codes if any.

8.4.6 Patient Object

A patient is a person who is receiving care. This resource covers Demographics and other administrative information about a patient.

The specifications are based on FHIR. Required fields are the minimum data to Create/Update a Patient Object. Patient Matching can be found in internal documentation.

Type	Attribute	Cardinality	Description	Optionality
identifier		1..*	Identifier Object	
	value		Edge systems must send a patient identifier that uniquely identifies the patient in the Edge System. Edge systems can also send Strong Identifiers like Drivers License, SSN, Passport. Each Strong identifier must have a defined Identifier Type.	R
	system		Assigning Authority ID for the unique Patient ID must be defined during the onboarding process. An Identifier value must have an identifier system that defines the Identifier.	R
	use		https://hl7.org/fhir/R4/valueset-identifier-use.html The primary patient ID used will always have identifier.use = “official”.	
	type		https://hl7.org/fhir/R4/valueset-identifier-type.html The following Identifier Types are considered Strong Identifiers and used for Patient Matching: SS: Social Security Number DL: Drivers License Number PPN: Passport Number	
	assigner		Organization that issued/manages the identifier	
	period.start		DateTime; The start of the period. The boundary is inclusive.	
	period.end		DateTime; The end of the period. If the high is missing, it means that the period is ongoing.	
active		0..1	Whether this patient's record is in active use When a Patient is deleted, this flag will be set as Inactive. 1: Active 0: Inactive Patients deleted will not be returned when retrieving matches. Default value is Active	
name		1..*	Display value Note: Historical names will be returned for GET	

			Probable Links by Patient ID	
	given		First name and Middle Name	R
	family	1..1	Last name or Surname *Please Note:* While we do support an array allowing for multiple values such as a married last name and a maiden last name, we do ask that it not be used for historical names but instead a separate object for each.	R
	prefix			
	suffix			
	use		https://hl7.org/fhir/R4/valueset-name-use.html	
	period.start		Time period when name was/is in use	
	period.end			
	text		FullName of the Patient	
gender		0..1	Administrative Gender https://hl7.org/fhir/R4/valueset-administrative-gender.html Values: M: Male, F: Female, O: Other, U: Unknown Administrative Sex in USCDI. We recommend that all new members follow the standard FHIR codes. In addition to the standard FHIR codes, 'UN: Undifferentiated" and "UNK: Unknown" are supported to maintain backwards compatibility.	O
birthDate		1..1	Format yyyy-mm-dd Required Data	R
address		1..*	Address Line Note: Historical addresses will be returned for GET Patient Links by Patient ID and GET Probable links by Patient ID.	
	line		Address line	R if known
	city			R if known
	state			R if known
	postalCode		Formats: • ##### • #####-#### • #########	R
	use		https://hl7.org/fhir/R4/valueset-address-use.html Home Old	

			‘Old’ addresses will be maintained in MPI and considered for patient matching.	
	period.start			
	period.end			
	type		https://hl7.org/fhir/R4/valueset-address-type.html	
telecom	value	0..*	Support phone numbers between 7-15 digits	
	system		https://hl7.org/fhir/R4/valueset-contact-point-system.html	
	use		https://hl7.org/fhir/R4/valueset-contact-point-use.html	
	period.start			
	period.end			
managingOrganization		1..1	Organization that is the custodian of the patient record	
	identifier object		Unique Value (Internal)	
	name			
link		0..*	Links to a Patient or RelatedPerson resource that concerns the same actual individual	
	other		The other patient or related person resource that the link refers to	
	type		“replaced-by” – for Merge Patients; the link refers to the Active Patient. The patient resource containing this link is the non-surviving patient https://hl7.org/fhir/R4/valueset-link-type.html	
disclosure.network		0..*	Please refer to the Network List	
	purposeofUse.code	1..1	Please refer to the POU codes listed per Network	
	purposeofUse.disclosureValue	1..1	1: Allowed (records will be shared) 0: Denied (records will not be shared)	
consentToDisclose		0..1	True: Will disclose records based on organization’s network settings (default) False: Will not disclose records for treatment and operations, but will disclose for other POU	

Patient Object Request Example

```
{
    "identifier": [
        {
            "value": "601",
            "period": {
```

```
                "start": "2010-09-12"
            },
            "system": "2.16.840.1.113883.3.2611.9.99.101.1",
            "use": "official"
        }
    ],
    "address": [
        {
            "line": [
                "511 Main St"
            ],
            "city": "Kingston",
            "state": "NY",
            "postalCode": "12401",
            "use": "home",
            "type": "both",
            "period": {
                "start": "2010-09-12"
            }
        }
    ],
    "birthDate": "1969-10-24",
    "gender": "M",
    "name": [
        {
            "family": [
                "Anderson"
            ],
            "given": [
                "David"
            ],
            "text": "David Anderson",
            "prefix": [
                "Mr"
            ],
            "suffix": [],
            "use": "usual",
            "period": {
                "start": "2010-09-12"
            }
        }
    ],
    "telecom": [
        {
            "system": "phone",
            "use": "home",
            "value": "(222) 222 2228",
            "period": {
                "start": "2010-09-12"
            }
```



```
        }
    ],
    "active": true
}
```

8.4.7 Patient Collection

A resource containing a collection of Patients and their respective Links, a collection of links available to the Edge System against the requested Patient resource given its current state.

Patients	1...*	Collection of Patients
Links	1..*	Collection of links related to the Patient resource {Self, PatientLink, Link, Unlink, ResetLink, Delete, ProbableLink)
Disclosure	0..*	
Patient	1..1	Patient Identifier(s), Patient Name, Address, DOB, gender, Telecom, Active

8.4.8 Status Object

Representation of both Error and Success codes and messages.

message	A brief description that describes the outcome of the requested action.
code	A unique code for the success or error response.

Response Status Example

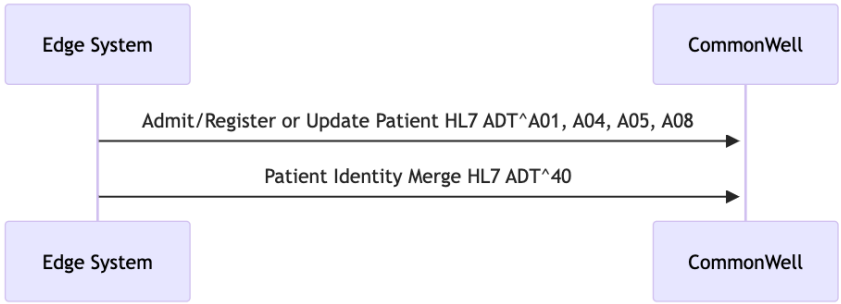
```
{
    "message": "Required field(s) missing: first and last name.",
    "code": 400
}
```

8.4.9 Patient Query Fields

Field	Description
Given	Patient First Name
Family	Patient Last Name
DOB	Date of Birth
Gender	Patient Gender
PostalCode	Patient Postal Code
IdentifierValue	Identifier Value
IdentifierSystem	Identifier System

9 Patient Identity Management Services (PIX)

This section describes a CommonWell PIX v2.x service, which is offered as an alternative for HIT vendors to the REST-based services for Patient Identity Management described in Section 8.3. The conforming message events are summarized in the diagram below:



9.1 Message Constraints

Messages MUST follow version 2.3.1 (or higher) of the HL7 Specification. The primary messaging constraints for HL7 messages are listed below.

- All messages MUST include MSH, EVN and PID segments.
- Segments PV1,PV2, and PD1 are optional.
- The MSH segment MUST include MSH-1, MSH-2, MSH-3, MSH-4, MSH-5, MSH-6, MSH-7, MSH-9 and MSH-10.
- MSH-1 MUST have the value “|”.
- MSH-2 MUST have the value “^~\&”.
- MSH-5 MUST have the specified receiving application value.
    - This value must match the organization configuration in the Management Portal
    - The primary AAID must be unique across all CommonWell orgs.
- MSH-6 MUST have the specified receiving facility value.
    - This value must match the organization configuration in the Management Portal.
- The message MUST include only one identifier in the PID-3 and that identifier MUST be a unique identifier in the Patient Identifier Domain and will be globally unique.
- For add and update messages, the PID segment MUST include PID-5, PID-7,and PID-11 (Postal Code).
- PD1-12 (Protection Indicator) to indicate whether the patient’s record should be disclosed in Get Patient Links.
    - If PD1-12 = Y, the record will not be disclosed
    - If PD1-12 = N, the record will be disclosed
    - By default, the patient record disclosure behavior is based on the organization’s network and purpose of use settings.
- For A40 merge messages, there MUST be only one identifier in MRG-2, and that identifier MUST be a unique identifier in the Patient Identifier Domain.
- All date and time fields MUST include UTC offset if the local time is used; otherwise it will be treated as UTC.

The codes that may be returned in the message acknowledgement are summarized below:

MSA-1	Description
AA	Application acknowledgment: Accept
AE	Application acknowledgement: Error

The acknowledgment is sent when the message is received.

Sample ADT message (A01)

```
MSH|^~\&|Resonance^2.16.840.1.113883.3.13.3.3^ISO|Cli_Facility|CW_App|CW_Facility|2013070809
44||ADT^A01|5616|D|2.5 EVN|A01|200711060941
PID|1||4933^^^&1.3.6.1.4.1.29928&ISO||Nolan^Frank||19450924|M|||8123 Hawthorne
Ave^^Chicago^IL^60612^US^P^042||(708)555-1234|(312)555-3456|E^ENGLISH^CLAN
PD1||||15014^Geiger^Jeffrey
```

Sample Acknowledgement (ACK) Message

```
MSH|^~\|CW_App|CW_Facility|Resonance^2.16.840.1.113883.3.13.3.3^ISO|Cli_Facility|20110104094
1||ADT^A01|5616|D|2.5 MSA|AA|0
```

9.2 Patient Add and Update

In response to patient admission, registration or update events, an Edge System acting as a Patient Identity Source Actor MUST respond by sending one of the following Admit/Register or Update messages to the CommonWell server acting as a Patient Identity Cross-reference Manager:

- A01 – Admission of an inpatient into a facility
- A04 – Registration of an outpatient for a visit of the facility
- A05 – Pre-admission of an inpatient (i.e., registration of patient information ahead of actual admission)

Changes to patient demographics (e.g., change in patient name, patient address, etc.) SHALL trigger the following Admit/Register or Update message:

- A08 – Update Patient Information

This message shall use the field PID-3 Patient Identifier List to convey the Patient ID uniquely identifying the patient within a given Patient Identification Domain.

9.3 Patient Transfer and Discharge

In response to patient transfer and discharge events, an Edge System acting as a Patient Identity Source Actor MUST respond by sending one of the following Transfer or Discharge messages to the CommonWell server acting as a Patient Identity Cross-reference Manager:

- A02 – Transfer of a patient between facilities
- A03 – Discharge of a patient from a facility

Changes to a patient's status as an inpatient or outpatient SHOULD trigger one of the following Transfer messages:

- A06 – Change an Outpatient to an Inpatient
- A07 – Change an Inpatient to an Outpatient

This message SHALL use the field PID-3 Patient Identifier List to convey the Patient ID uniquely identifying the patient within a given Patient Identification Domain.

The system only looks at the patient demographics in the PID-3 Patient Identifier segment to uniquely identify and update the patient. If the message matches to an existing patient, only the demographic information in from the most recent message is maintained.

9.4 Patient Merge

When two Patient Records are found to identify the same patient in a Patient Identity Domain, an Edge System, acting as a Patient Identity Source Actor, MUST respond by sending the appropriate ADT merge event notification to the CommonWell server acting as the Patient Identity Cross-reference Manager:

- A40 – Merge Patient – Internal ID

An A40 message indicates that the Patient Identity Source Actor has merged Patient Records within a specific Patient Identification Domain. That is, MRG-1 (Patient ID) has been merged into PID-3 (Patient ID).

10 CHA Data Broker

This document describes how Edge Systems will use the CommonWell Data Broker to retrieve documents from other Edge Systems. Service Adopters can decide whether to use REST or IHE to accomplish document exchange.

10.1 REST API Reference

CommonWell provides REST services that support workflows facilitating document exchange in the network with other Edge systems.

10.2 FHIR US Core

All FHIR endpoints are expected to be US Core compliant. These specifications are based on existing CW documentation and may be changed upon further review.

Supported search parameters FHIR DocumentReference:

Parameter	Description
Patient.identifier	ID of who/what is the subject of the document
author.given	Given name of who and/or what authored the document
author.family	Family name of who and/or what authored the document
status	current | superseded | entered-in-error
period	Time of service start that is being documented. Comparators: ge
period	Time of service end that is being documented. Comparators: le
date	When the document reference was created. Comparators: ge
date	When the document reference was created. Comparators: le
contenttype	Mime type of the content, with charset etc. Please note that this parameter is not supported in IHE. This filter would only apply to FHIR responders. IHE responders will not apply this filter.
documenttype	Kind of document, e.g. LOINC

10.2.1 Document Query

Document query is a user-or system-initiated query to determine whether a specific patient has a record at other Edge system locations. This query is used to find DocumentReference resources satisfying provided query parameters, and the result of the query is a bundle of DocumentReference resources that match the query parameters.

GET /v2/R4/DocumentReference?patient.identifier=<code-system>|<value>	

Parameters	• patient.identifier – assigning authority identifier and patient identifier pipe delimited
	• Status - The DocumentReference status (in XDS nomenclature, the availability status of the submission set) to filter by. Valid values are listed below:
	  ○ current
	  ○ Superceded
	  ○ entered-in-error

	Example: /v2/R4/DocumentReference?patient.identifier=2.16.840.1.113884.3.101.1|patient123
Request Body	N/A for HTTP GET requests

Response	{
	"resourceType": "Bundle",
	"entry": [
	{
	"fullUrl":
	"https://api.integration.commonwellalliance.lkopera.com/v2/R4/Binary/eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9",
	"resource": {
	"resourceType": "DocumentReference",
	"category": [
	{
	"coding": [
	{
	"code": "clinical-note",
	"display": "Clinical Note",
	"system":
	"http://hl7.org/fhir/us/core/CodeSystem/us-core-documentreference-category"
	}
	]
	}
	],
	"content": [
	{
	"attachment": {
	"url":
	"https://api.integration.commonwellalliance.lkopera.com/v2/R4/Binary/eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9"
	},
	"format": {
	"code":
	"urn:ihe:iti:xds:2017:mimeTypeSufficient",
	"display": "mimeType Sufficient",
	"system":
	"http://ihe.net/fhir/ValueSet/IHE.FormatCode.codesystem"
	}
	}
	],
	"masterIdentifier": {
	"value":
	"eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9"
	},
	"status": "current",
	"subject": {
	"identifier": {

	<pre>"assigner": {
	"reference": "Oswego Health System"
	},
	"value": "22198911"
	}
	}
	}
	},
	...
	]
	}</pre>

Documents need to have the following fields:
DocumentReference.Content.Attachment.ContentType = Mimetype
DocumentReference.Content.URL = DocumentID

10.2.2 Document Retrieve

Document Retrieve is the process of retrieving a specific document or set of documents related to a patient. After Document Query, where a query is first sent to from a specific system to determine the existence of the document, and the retrieve operation is performed to access the document. The retrieve operation involves sending an HTTP GET request to the server using the location value obtained from the query response.

GET <DocumentReference.content.attachment.url>	
Parameters	
Request Body	

Response	<pre>{
	"resourceType": "Binary",
	"contentType": "application/rtf",
	"data": "e1xydGYxXGFuc2lcZGVm.....", *//base 64 encoded*
	"id": "Binary/
	eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJ
	IY0lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1BhdE
	lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5M
	DAiLCJUUGF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9
	",
	}</pre>

Notes for Document Contributors
Documents need to have the following fields:
Binary.Contenttype.Attachment.ContentType = Mimetype
Binary.data = DocumentID

10.2.3 Patient Match

This allows us to do a patient search that retrieves patient matches.

https://{CommonwellEnvUrl}/v2/R4/Patient/$match	
Parameters	

Request Body	<pre>"parameter": [
	        {
	           "name": "resource",
	      "resource": {
	            "resourceType": "Patient",
	            "id": "{AAID}|{PatientID}"
	       }
	        }
	    ],
	    "resourceType": "Parameters"
	}</pre>

Response	<pre>{
	  "resourceType": "Bundle",
	  "type": "searchset",
	  "total": 1,
	  "entry": [
	    {
	      "fullUrl": "https://fhirserver.com/R4/Patient/{id}",
	      "resource": {
	        "resourceType": "Patient",
	        "id": "{id}",
	        "managingOrganization": {
	          "reference": "Organization/{orgId}",
	          "display": "{orgName}"
	        }
	      }
	    },
	    {
	      "fullUrl": "https://fhirserver.com/R4/Organization/{orgId}",
	      "resource": {
	        "resourceType": "Organization",
	        "id": "{orgId}",
	        "name": "{orgName}",
	        "address": [
	          {
	            "line": ["456 Clinic Drive"],
	            "city": "Anytown",
	            "state": "CA",
	            "postalCode": "90210",
	            "country": "USA"
	          }
	        ]
	      "endpoint": {
	           "reference": "Endpoint/5a0a1f4c-1b37-4bd8-9b3a-
	3c834969a723"
	        }</pre>

	<pre>}
	}
	]
	}</pre>

10.3 XCA

Supported search parameters for XCA Query:

Parameter	Description
$XDSDocumentEntryPatientId	ID of who/what is the subject of the document
$XDSDocumentEntryAuthorPerson	Who and/or what authored the document
$XDSDocumentEntryStatus	urn:oasis:names:tc:ebxml-regrep:StatusType:Approved | urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated | urn:ihe:iti:2010:StatusType:DeferredCreation
$XDSDocumentEntryServiceStopTimeFrom	Time of service start that is being documented.
$XDSDocumentEntryServiceStopTimeTo	Time of service end that is being documented.
$XDSDocumentEntryCreationTimeFrom	When the document reference was created.
$XDSDocumentEntryCreationTimeTo	When the document reference was created.
$XDSDocumentEntryType	Kind of document, e.g. LOINC

10.3.1 XCA Query

XCA query is a query for documents using the Cross-Community Access (XCA) profile, which is a standard for querying and retrieving patient documents across different healthcare communities.

POST /v2/XCA/Query	
Parameters	$XDSDocumentEntryPatientId slot – contains the assigning authority identifier and patient identifier in the Hl7 ISO format $XDSDocumentEntryStatus

Request Body	<pre><Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.w3.org/2003/05/soap-envelope">
	<Header />
	<Body>
	<AdhocQueryRequest xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0">
	<AdhocQuery xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
	<Slot name="$XDSDocumentEntryPatientId">
	<ValueList>
	<Value>
	22198900^^^&2.16.840
	.1.113883.3.2611.9.99.10
	2.1&ISO
	</Value>
	</ValueList>
	</Slot>
	<Slot name="$XDSDocumentEntryStatus">
	<ValueList>
	<Value>
	urn:oasis:names:tc:ebxml
	-</pre>

	regrep:StatusType:Approved </Value> </ValueList> </Slot> </AdhocQuery> </AdhocQueryRequest> </Body> </Envelope>
Response	<Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.w3.org/2003/05/soap-envelope"> <Body> <AdhocQueryResponse status="status" xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"> <RegistryObjectList xmlns="urn:oasis:names:tc:ebxml- regrep:xsd:rim:3.0"> <ExtrinsicObject home="urn:oid:2.16.840.1.113883.3.2611.9.99 .101" id="eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQ wIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi44ND AuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1Bhd ElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjku OTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJPc3d lZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9" isOpaque="false" objectType="urn:uuid:7edca82f-054d-47f2- a032-9b2a5b5186c1" status="urn:oasis:names:tc:ebxml- regrep:StatusType:Approved"> <Slot name="repositoryUniqueId"> <ValueList> <Value>r4</Value> </ValueList> </Slot> <Slot name="size"> <ValueList> <Value>False</Value> </ValueList> </Slot> <Slot name="sourcePatientId"> <ValueList> <Value>T1- 22198900^^^&Oswego Health System&ISO</Value> </ValueList> </Slot> <Classification classificationScheme="urn:uuid:41a5887f- 8865-4c09-adf7-e362475b143a" classifiedObject="eyJEb2NJZCI6IkJpbmFyeS9wY XRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lk IjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTk uMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4OD MuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUU GF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0y MjE5ODkwMCJ9" id="urn:uuid:375d4571-8370- 4724-b3c9-3c4b2a3833ed"

```
nodeRepresentation="clinical-note"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classifica
tion">
      <Slot name="codingScheme">
            <ValueList>
                  <Value>http://hl7.org/fh
                  ir/us/core/CodeSystem/us
                  -core-documentreference-
                  category</Value>
            </ValueList>
      </Slot>
      <Name>
            <LocalizedString charset="UTF-
            8" value="Clinical Note"
            xml:lang="en-US" />
      </Name>
</Classification>
<Classification
classificationScheme="urn:uuid:a09d5840-
386c-46f2-b5ad-9c3699a4309d"
classifiedObject="eyJEb2NJZCI6IkJpbmFyeS9wY
XRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lk
IjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTk
uMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4OD
MuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUU
GF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0y
MjE5ODkwMCJ9" id="urn:uuid:87dab2f9-de6a-
4af9-b284-9e0ee94e0e9f"
nodeRepresentation="urn:ihe:iti:xds:2017:mi
meTypeSufficient"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classifica
tion">
      <Slot name="codingScheme">
            <ValueList>
                  <Value>http://ihe.net/fh
                  ir/ValueSet/IHE.FormatCo
                  de.codesystem</Value>
            </ValueList>
      </Slot>
      <Name>
            <LocalizedString charset="UTF-
            8" value="mimeType Sufficient"
            xml:lang="en-US" />
      </Name>
</Classification>
<Classification
classificationScheme="urn:uuid:f0306f51-
975f-434e-a61c-c59651d33983"
classifiedObject="eyJEb2NJZCI6IkJpbmFyeS9wY
XRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lk
IjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTk
uMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4OD
MuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUU
GF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0y
MjE5ODkwMCJ9" id="urn:uuid:f3412186-a34c-
4bd7-b2ef-a4cd7153f17f"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classifica
tion">
```

```
      <Slot name="codingScheme">
            <ValueList>
                  <Value />
            </ValueList>
      </Slot>
</Classification>
<Classification
classificationScheme="urn:uuid:f4f85eac-
e6cb-4883-b524-f2705394840f"
classifiedObject="eyJEb2NJZCI6IkJpbmFyeS9wY
XRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lk
IjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTk
uMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4OD
MuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUU
GF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0y
MjE5ODkwMCJ9" id="urn:uuid:132a396b-c3bc-
4692-adad-4d27cbe6967d"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classifica
tion">
      <Slot name="codingScheme">
            <ValueList>
                  <Value />
            </ValueList>
      </Slot>
</Classification>
<Classification
classificationScheme="urn:uuid:f33fb8ac-
18af-42cc-ae0e-ed0b0bdb91e1"
classifiedObject="eyJEb2NJZCI6IkJpbmFyeS9wY
XRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lk
IjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTk
uMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4OD
MuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUU
GF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0y
MjE5ODkwMCJ9" id="urn:uuid:b390d94e-5364-
4ae7-b808-2a7e72aefab4"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classifica
tion">
      <Slot name="codingScheme">
            <ValueList>
                  <Value />
            </ValueList>
      </Slot>
</Classification>
<ExternalIdentifier id="urn:uuid:1081128a-
350d-440f-9ee2-ea05b2367f37"
registryObject="eyJEb2NJZCI6IkJpbmFyeS9wYXR
pZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIj
oiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuM
TAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMu
My4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF
0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMj
E5ODkwMCJ9"
identificationScheme="urn:uuid:2e82c1f6-
a085-4c72-9da3-8640a32e42ab"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalId
entifier"
value="eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90
```



```
                                ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi4
                                4NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1
                                BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExL
                                jkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJP
                                c3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ
                                9">
                                      <Name>
                                            <LocalizedString charset="UTF-
                                            8"
                                            value="XDSDocumentEntry.unique
                                            Id" xml:lang="en-US" />
                                      </Name>
                                </ExternalIdentifier>
                                <ExternalIdentifier id="urn:uuid:22fbd396-
                                1d4b-4bdb-bd05-f7272d47ab38"
                                registryObject="eyJEb2NJZCI6IkJpbmFyeS9wYXR
                                pZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIj
                                oiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuM
                                TAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMu
                                My4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF
                                0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMj
                                E5ODkwMCJ9"
                                identificationScheme="urn:uuid:58a6f841-
                                87b3-4a3e-92fd-a8ffeff98427"
                                objectType="urn:oasis:names:tc:ebxml-
                                regrep:ObjectType:RegistryObject:ExternalId
                                entifier" value="T1-22198900^^^&amp;Oswego
                                Health System&amp;ISO">
                                      <Name>
                                            <LocalizedString charset="UTF-
                                            8"
                                            value="XDSDocumentEntry.patien
                                            tId" xml:lang="en-US" />
                                      </Name>
                                </ExternalIdentifier>
                                </ExtrinsicObject>
                                <ExtrinsicObject
                                home="urn:oid:2.16.840.1.113883.3.2611.9.99
                                .101"
                                id="eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQ
                                xIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi44ND
                                AuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1Bhd
                                ElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjku
                                OTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJPc3d
                                lZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9"
                                isOpaque="false"
                                objectType="urn:uuid:7edca82f-054d-47f2-
                                a032-9b2a5b5186c1"
                                status="urn:oasis:names:tc:ebxml-
                                regrep:StatusType:Approved"> ....
                                </ExtrinsicObject>
                          </RegistryObjectList>
                    </AdhocQueryResponse>
              </Body>
</Envelope>
```

10.3.2 XCA Retrieve

XCA retrieve is the process of retrieving patient documents using the Cross-Community Access (XCA) profile performed after the XCA Query for documents.

POST /v2/XCA/Retrieve	
Parameters	• HomeCommunityId – home community identifier of the targeted system • RepositoryUniqueId – repository identifier • DocumentUniqueId – unique identifier of the document
Request Body	<Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.w3.org/2003/05/soap-envelope"> <Header /> <Body> <RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007"> <DocumentRequest> <HomeCommunityId>urn:oid:2.16.840.1.113883.3.2611.9.99.101</HomeCommunityId> <RepositoryUniqueId>r4</RepositoryUniqueId> <DocumentUniqueId>eyJEb2NJZCI6IkJpbmFyeS9wYXRpZW50bm90ZTQwIiwiUmVwb0lkIjoicjQiLCJIY0lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAxIiwiU1BhdElkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy4yNjExLjkuOTkuMTAyLjF8MjIxOTg5MDAiLCJUUGF0SWQiOiJPc3dlZ28gSGVhbHRoIFN5c3RlbXxUMS0yMjE5ODkwMCJ9</DocumentUniqueId> </DocumentRequest> </RetrieveDocumentSetRequest> </Body> </Envelope>
Response	<Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.w3.org/2003/05/soap-envelope"> <Body> <RetrieveDocumentSetResponse xmlns="urn:ihe:iti:xds-b:2007"> <DocumentResponse> <RepositoryUniqueId>r4</RepositoryUniqueId> <DocumentUniqueId>Binary/patientnote40</DocumentUniqueId> <mimeType>application/rtf</mimeType> <Document> <Include href="cid:Binary/patientnote40" xmlns="http://www.w3.org/2004/08/xop/include" /> </Document> </DocumentResponse> </RetrieveDocumentSetResponse> </Body> </Envelope>
Multipart HTTP Response	Content-Type: application/xop+xml; charset=utf-8; type="application/soap+xml" Content-ID: <97e1cc69-4e63-4d52-bb3a-6b45f9043162> Content-Transfer-Encoding: binary <s:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/" xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"

	xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <s:Body> <RetrieveDocumentSetResponse xmlns="urn:ihe:iti:xds-b:2007"> <DocumentResponse> <RepositoryUniqueId>r4</RepositoryUniqueId> <DocumentUniqueId>Binary/patientnote40</DocumentUniqueId> <mimeType>application/rtf</mimeType> <Document> <Include href="cid:Binary/patientnote40" xmlns="http://www.w3.org/2004/08/xop/include"/> </Document> </DocumentResponse> </RetrieveDocumentSetResponse> </s:Body> </s:Envelope> Content-Type: application/rtf Content-ID: <Binary/patientnote40> Content-Transfer-Encoding: binary {\rtf1\ansi\deff0{\fonttbl{\f0\fswiss\fprq2\fcharset0 Calibri;}} \viewkind4\uc1\pard\lang9\b\f0\fs22 Visit Detail\par \par Chart #: 065AA60EE4\par Patient Name: Mikebot, Salbot \par Date of Birth: 04/17/1961\par \par Encounter ID: 127693_80099279_ER_0001739051\par Encounter Date: 01/01/1900\par Encounter Title: \par Encounter Type: \par Attending Doctor: Casperbot, Carlbot \par }

10.3.3 Targeted XCA Query

Targeted XCA query is the process of sending a document query using the Cross-Community Access (XCA) profile but only retrieving from specific organizations.

To use this feature, in the ITI-38, populate the home value with the organization ID that you want to query. In the query, send the local patient id from your own system, not the one in the target system.

Please note that ITI-18 is not supported. If the home value is not populated, the home value is populated with the Broker/CommonWell's OID, or the home value is the organization's own ID, then the Broker does the full CommonWell fanout.

Request Body	<Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.w3.org/2003/05/soap-envelope"> <Header /> <Body> <AdhocQueryRequest xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"> <rim:AdhocQuery home="target.system.to.search.oid"> <rim:Slot name="$XDSDocumentEntryPatientId"> <rim:ValueList>

	<rim:Value>DemoChart115^^^&2.16.840.1.113883.3.2611.9.99.102.1&ISO</rim:Value> </rim:ValueList> </rim:Slot> <rim:Slot name="$XDSDocumentEntryStatus"> <rim:ValueList> <rim:Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')</rim:Value> </rim:ValueList> </rim:Slot> </rim:AdhocQuery> </AdhocQueryRequest> </Body> </Envelope>

11 Patient Access Data Requests

The Patient Access Use Case outlines two scenarios under which a patient/consumer may query for their own clinical data: nonHIPAA related Individual Access Services (IAS) and HIPAA related IAS. The technical requirements outlined below are specific to the nonHIPAA related IAS.

To interact with CommonWell, the patient MUST be ID proofed by a third-party identity proofing service to a level IAL2 or greater. IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2[5] (AAL2) requirements. Once the patient has been ID proofed, they will be allowed access to the CommonWell network through registration and autolinking as well as targeted patient match transactions. After the patient has been matched at their existing care locations the patient will have access to their clinical documents through the query and retrieve transactions. All transactions with a REQUEST purpose of use will require verification that the patient has been ID proofed through an ID proofing receipt that can be audited with each transaction.

11.1 Identity Proofing

All individuals that access CommonWell using nonHIPAA related IAS are expected to have their demographic data verified by a third-party identity proofing service that is Kantara certified to NIST IAL2 or greater. IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2[5] (AAL2) requirements. All demographic data that is provided in the patient registration transaction MUST only contain verified data. Anytime demographic data, primary address, contact information is modified in IAS app, they must be verified by the ID proofing service prior to adding or updating the information in CommonWell.

11.1.1 Alternative Identifier

To verify that the person has been ID proofed by an identity proofing service, CommonWell requires that an Alternative Identifier be provided representing the unique ID receipt from the identity proofing transaction. The Alternative Identifier will be composed of a unique key along with the OID of the identity proofing vendor.

This Alternative Identifier is expected to be provided on the patient registration and any subsequent patient update transactions as a secondary identifier within the Patient Resource. For more information, refer to the following section of this document: 8.2.3 Secondary or Alternate ID.

Example


```
{
 "_links": "link relations",
 "active": true,
 "provider": {
  "type": "Organization",
  "reference": "https://rest.api.commonwellalliance.org/v1/org/2.16.840.1.113883.3.4/",
  "display": "Oswego Health System"
 },
 "identifier": [{
    "use": "official",
    "type": "MR",
    "value": "9876",
    "system": "2.16.840.1.113883.3.4",
    "assigner": "Oswego Health System"
  },
  {
    "use": "secondary",
```



```
    "type": "IAL2",
    "value": "TU-1234",
    "system": "1.20.4.18.35.2.60.12.64.3.1.72713.1",
    "assigner": "TransUnion"
   }],
  "details": {
   "name": [{
     "given": ["Frank"],
     "family": ["Nolan"]
    }],
   "address": [{
     "zip": "60610",
     "state": "Il",
     "line": ["511 Oswego St"],
     "city": "Chicago"
    }],
  "gender": {
   "system": "http://hl7.org/fhir/vs/administrative-gender",
   "code": "M"
  },
  "birthDate": "1945-09-24"
}
```

11.1.1.1 AlternatePatients for validated attributes

The alternatePatients field can be used to distinguish validated attributes returned by the third-party identity proofing service from the “regular” patient attributes, and may be required for other uses cases such as TEFCA Individual Access (See 11.1.1.3 – TEFCA Individual Access Services).

An alternatePatientPatients.identifier must match a patient.identifer in the main patient object.

AlternativePatients is an array so that users can add the attributes specific to each alternate ID.

Example Patient Object with the alternativePatients

```
{
        "identifier": [
                {
                        "value": "601",
                        "period": {
                                "start": "2010-09-12"
                        },
                        "system": "2.16.840.1.113883.3.2611.9.99.101.1",
                        "use": "official",
                        "assigner": "Example Health System"
                },
                {
                        "value": "TU-1234",
                        "system": "1.20.4.18.35.2.60.12.64.3.1.72713.1",
                        "use": "secondary",
                        "type": "IAL2",
                        "assigner": "TransUnion"
```

```
        }
    ],
    "address": [
        {
            "line": [
                "511 Main St"
            ],
            "city": "Kingston",
            "state": "NY",
            "postalCode": "12401",
            "country": "USA",
            "use": "home",
            "type": "both",
            "period": {
                "start": "2010-09-12"
            }
        }
    ],
    "birthDate": "1969-10-24",
    "gender": "M",
    "name": [
        {
            "family": [
                "Anderson"
            ],
            "given": [
                "David"
            ],
            "text": "David Anderson",
            "prefix": [
                "Mr"
            ],
            "suffix": [],
            "use": "usual",
            "period": {
                "start": "2010-09-12"
            }
        }
    ],
    "telecom": [
        {
            "system": "phone",
            "use": "home",
            "value": "(222) 222 2228",
            "period": {
                "start": "2010-09-12"
            }
        }
    ],
    "active": true,
    "maritalStatus": {
        "code": "M",
        "display": "Married"
```



```
},
"alternatePatients": [
        {
                "identifier": [
                        {
                                "value": "TU-1234",
                                "system": "1.20.4.18.35.2.60.12.64.3.1.72713.1",
                                "use": "secondary",
                                "type": "IAL2",
                                "assigner": "TransUnion"
                        }
                ],
                "address": [
                        {
                                "line": [
                                        "511 Main St"
                                ],
                                "city": "Kingston",
                                "state": "NY",
                                "postalCode": "12401",
                                "country": "USA",
                                "use": "home",
                                "type": "both",
                                "period": {
                                        "start": "2010-09-12"
                                }
                        }
                ],
                "birthDate": "1969-10-24",
                "gender": "M",
                "name": [
                        {
                                "family": [
                                        "Anderson"
                                ],
                                "given": [
                                        "David"
                                ],
                                "text": "David Anderson",
                                "prefix": [],
                                "suffix": [],
                                "use": "",
                                "period": {}
                        }
                ],
                "telecom": [
                        {
                                "system": "phone",
                                "use": "home",
                                "value": "(222) 222 2228",
                                "period": {}
                        }
                ],
```



```
                "active": true,
                "maritalStatus": {
                        "code": "M",
                        "display": "Married"
                }
        }
    ]
}
```

11.1.1.2 Alternate Assigning Authority Configuration

To allow the use of the alternative identifier on the patient, the untethered-PHR will need to configure an alternate assigning authority for its organization. This alternate assigning authority will be the OID of the identity proofing vendor used by the untethered-PHR.

The alternate assigning authority must match a secondary AAID in the patient object.

11.1.1.3 TEFCA Individual Access Services

CommonWell organizations that want to query TEFCA for Individual Access Services must add the validated attributes from the third-party identity proofing service to the alternatePatient field as evidence of identity proofing.

For TEFCA Individual Access Services, the minimum fields required for query initiation are First Name, Last Name, Date of Birth, Address, City, State, and Zip.

While TEFCA has a different POU code (T-IAS), CommonWell organizations will still use the CW NHIN POU code of REQUEST to query for TEFCA.

The IAS SOP has 2 versions. IAS v1 refers to the IAS SOP v1.0. IAS v2 refers to the IAS SOP v2.0 or 2.1. CommonWell supports both the versions. As of now, it is recommended to form your request conforming to both the versions to increase the request reach across QHINs. However, if you only support IAS v1, we will still support the request.

IAS v1 Implementation

For IHE

For initiating organization, the CHA Broker will check that the validated attributes in the SAML are present in the Patient object. An error will be returned if the required fields are missing or the SAML is malformed.

TEFCA uses the terminology credential service provider (CSP) to denote the third-party identity proofing vendor.

SAML example:

```
<saml:AttributeStatement>
                <...>
        <saml:Attribute Name="csp" NameFormat="">
                <saml:AttributeValue>http://www.example-csp.com</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="validated_attributes" NameFormat="">
```

```
            <saml:AttributeValue>lname,fname,address,city,state,email,ssn,sex
            </saml:AttributeValue>
        </saml:Attribute>
</saml:AttributeStatement>
```

Supported validate attributes:

Demographic	Code	Optionality
First Name	fname	R
Last Name	lname	R
Middle Name	mname	O
Middle Initial	minitial	O
Suffix	suffix	O
Date of Birth	dob	R
Sex	sex	O
Address	address	R
City	city	R
State	state	R
Zip/ZIP+4	zip	R
Phone Number	phone	O
Email Address	email	O
Social Security Number	ssn	O
SSN last 4 digits	ssn4	O
Medical Record Number	mrn	O
Identifier	identifier	O

For FHIR

The FHIR clients do not need to send any specific information, as the outgoing SAML will be built from the demographics already validated by the MPI component

IAS v2 Implementation

For IHE

The IAS provider must also include the IAL2 token granted to them by the CSP in the SAML attribute “id_token”

Example:

```
<saml2:Attribute Name="id_token">
       <saml2:Attribute NameFormat=”oasis:names:tc:SAML:2.0:cm:bearer”>
       <saml2:AttributeValue>{Base64 encoded token}</saml2:AttributeValue>
</saml2:Attribute>
```

For FHIR

If the IAS Provider primarily uses FHIR, they need to send this OIDC token in “id_token” claim under the “tefca_ias” extension.

Base64 Encoded Token in the JWT:

“extensions”:{

“tefca_ias”: {

“id_token”: “{Base64 Encoded Token}”

}

}

Example:

OIDC Token

{
"alg":"RS256",
"kid":"toW9jMUSN/5/L3iwaQGdTmNDuhvp/JcAZVH/RGF2aWQgUHlrZQ==",
"typ":"JWT"
}

{

"aud":"hci1",

"iat":1666280632,

"iss":"https://csp.example.com",

"sub":"f7bdf590-2fc4-4718-8f33-043c8f96b66d",

"jti":"bcb9533e-1cc1-48bd-848b-b4200ea504b9",

"given_name":"John",

"family_name":"Schmidt",

"middle_name":"Jacob Jingleheimer",

"nickname":"Ed",

"email":"jjjs@example.com",

"email_verified":true,

"phone_number":"555-555-5555",

"gender":"M",

"birthdate":"Unknown",

"address":{

"formatted":"1060 West Addison Street, Chicago, IL 60613 USA",

"street_address":"1060 West Addison Street",

"locality":"Chicago",

"region":"Illinois",

"postal_code":"60613",

"country":"USA"

},

"http://rce.sequoiaproject.org/OIDC/claim/mothers_maiden_name":"Vedder",
"http://rce.sequoiaproject.org/OIDC/claim/principle_care_provider_id":"2938457234",
"http://rce.sequoiaproject.org/OIDC/claim/birth_place_address": {

"formatted":"1060 West Addison Street, Chicago, Illinois 60613 USA",

"street_address":"1060 West Addison Street",

"locality":"Chicago",

"region":"Illinois",

"postal_code":"60613",

"country":"USA"

},

"historical_address":{

"formatted":"31 Spooner Street, Quahog, Rhode Island 02907",

"street_address":"31 Spooner Street",

"locality":"Quahog",

"region":"Rhode Island",

"postal_code":"02907",

"country":"USA"

},

"http://rce.sequoiaproject.org/OIDC/claim/birth_place_name":"Peaceful Valley Hospital"

}

Note:
The patient access workflow initiates with querying the patient with the appropriate purpose of use as

mentioned above. Please refer to the patient/$match (section 10.2.3) on how to initiate a query.

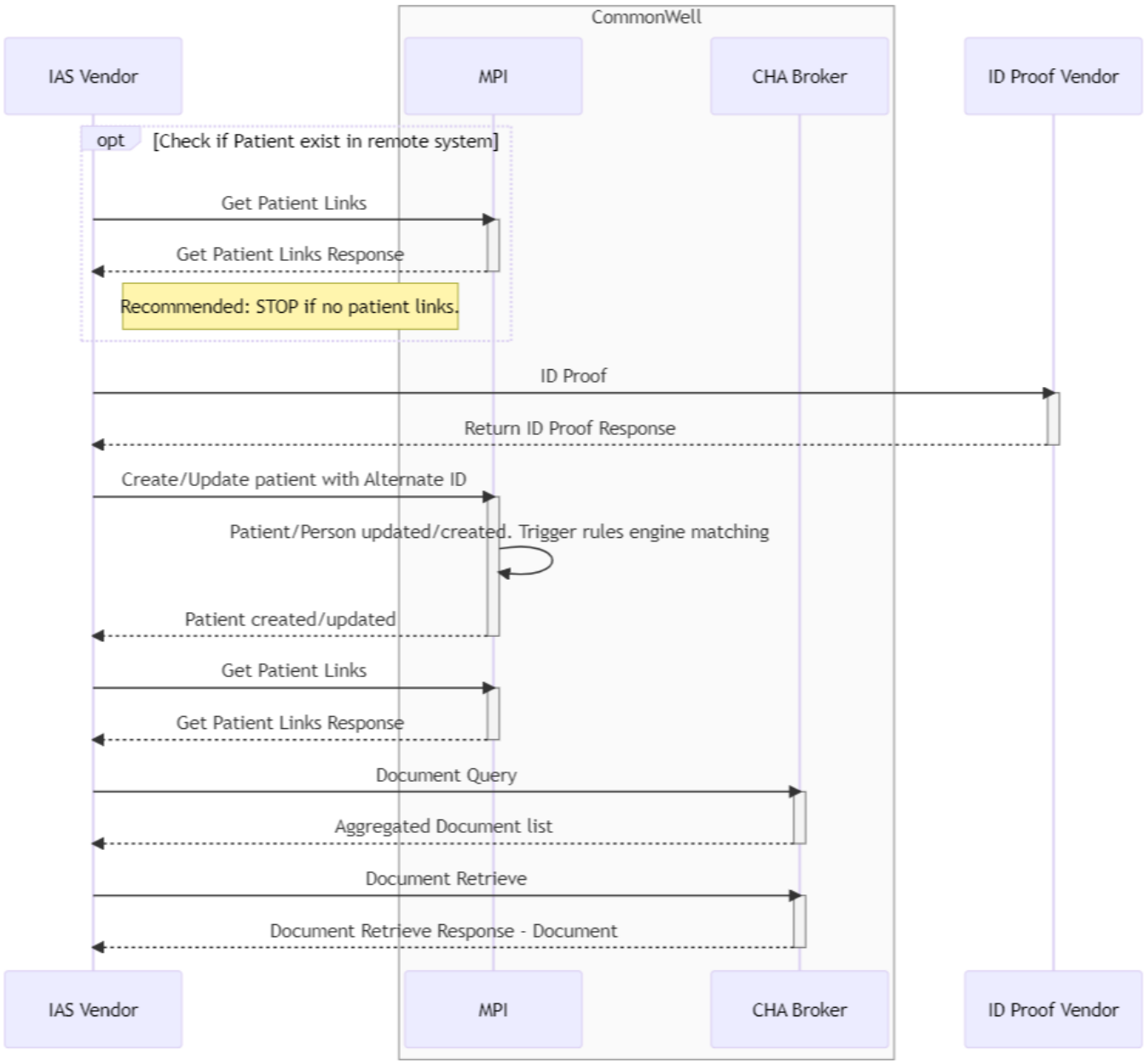
IAS with EPIC requires some steps in addition to the above workflow. You can find more details at the following location – https://open.epic.com/Home/Interoperate/TEFCA/IAS

11.2 Patient Registration

NonHIPAA related IAS will still follow the same workflow as the treatment use case where the patient needs to be registered in CommonWell. This is a standard workflow supported by CommonWell.

For more information, refer to the following sections of this document: Sections 8.3 and 9.2.

12.2.1 Workflow Patient Access Patient Registration/Enrollment Sequence Diagram



11.2.2 Checking for Potential Patient Matches Prior to ID Proofing and Patient Registration

Checking for whether patient matches exist prior to ID proofing is an OPTIONAL workflow. By providing the patient ID in the request, this transaction will indicate whether potential patient matches exist as well as the number of potential matches available for the patient. This could be utilized by the nonHIPAA related IAS to indicate whether they want to put the patient through their ID proofing process to gain access to the CommonWell network. For more information, see the following section in this document: 8.4.1 Get Patient Links.

11.3 Record Location and Linking

This section describes changes to existing record location and linking transactions for patient access requests.

11.3.1 REQUEST Purpose of Use changes

All linking for nonHIPAA related IAS patients SHALL be accomplished through either the autolinking process or links that are confirmed at a different care location (Refer to Get Patient Links). Manual linking via the probabilistic matching workflow MUST NOT be used for this use case (Refer to Get Probable Links).

11.3.1.1 Retrieve Network Links

Use Get Patient Links to return all confirmed (LOLA 2) patient matches which were generated though either autolinking or manually linking.

11.4 Document Query & Retrieve

CommonWell provides a centralized broker service for executing document query and retrieval transactions on behalf of edge systems to the various responding gateways participating within the CommonWell network. For more information, refer to the following section of this document: 10 CommonWell Health Alliance Broker (CHA Broker).

Appendix A – Terminology Bindings

The table below contains the terminology bindings used in this specification. For a full list of the FHIR terminology bindings, see http://hl7.org/fhir/R4/terminology-module.html.

Name	Definition	Type	Reference
AddressUse	The use of an address	Code List	https://hl7.org/fhir/R4/codesystem-address-use.html
AdministrativeGender	The gender of a person used for administrative purposes	Value Set	https://www.hl7.org/fhir/R4/valueset-administrative-gender.html
ContactSystem	What kind of contact this is	Code List	https://www.hl7.org/fhir/R4/valueset-contact-point-system.html
ContactUse	How to use this address	Code List	https://www.hl7.org/fhir/R4/valueset-contact-point-use.html
VisitClass	Classification of the visit	Code List	https://www.hl7.org/fhir/R4/v3/ActEncounterCode/vs.html
IdentifierUse	Identifies the use for this identifier, if known	Code List	https://hl7.org/fhir/R4/codesystem-identifier-use.html
MimeType	The mime type of an attachment	Reference	BCP 13 (RFCs 2045, 2046, 2047, 4288, 4289 and 2049) (http://www.rfc-editor.org/bcp/bcp13.txt)
NameUse	The use of a human name	Code List	https://hl7.org/fhir/R4/codesystem-name-use.html
PractitionerRole	The role a person plays representing an organization	Value Set	https://www.hl7.org/fhir/R4/valueset-practitioner-role.html

The specific value sets and code lists are also detailed in the following sections.

A.1 Administrative Gender Codes

This value set defines the set of codes that can be used to indicate the administrative gender of a person.

Code	Display	Definition
F	Female	Female
M	Male	Male
U	Unknown	Unknown
O	Other	Other

The API will accept either code or display value as long as it follows FHIR R4 or HL7 standards.

Undifferentiated (UN) and Unknown (UNK) is maintained for backwards compatibility

If an other value is used, the system will be stored as blank.

A.2 Patient Role and Purpose of Use Codes

These values are defined in the HITSP Clinical Document and Message Terminology Component (HITSP C80) version 2.0 found at https://ushik.ahrq.gov/portals/hitsp/reference_documents/HITSP_V2.0_2010_C80_-_Clinical_Document_and_Message_Terminology.pdf. The accepted codes are defined in Table 2-155 Author Role Value Set Definition.

Code	Display	Definition
see Table 2-155 for provider codes	any provider from Table 2-155 Author Role Value Set Definition	Treatment
116154003	patient	Patient Access
307785004	insurance specialist	Coverage

A.3 Purpose of Use Codes

Unless otherwise specifically noted, CommonWell Service Adopters are only required to use the NHIN Purpose of Use code set. The CHA Broker is responsible for correlating the corresponding codes to the corresponding external network purpose of use code set.

Refer to the Use Case specification for additional details regarding Permitted Purposes and the Purpose of Use codes.

Code	Description	Note
TREATMENT	Treatment	TEFCA supports two mutually exclusive treatment POU codes, T-TREAT and T-TRMNT. CW Service Adopters will still TREATMENT as the POU code to initiate queries, but responding will be dependent on the Org TEFCA configuration.
REQUEST	Patient Request/IAS	
PAYMENT	Payment	
OPERATIONS	Health Care Operations	
PUBLICHEALTH	Public Health	
COVERAGE	Government Benefits Determination	
T-PH-ECR	Electronic Case Reporting	Code supported for CW orgs participating in TEFCA
T-PH-ELR	Electronic Lab Reporting	Code supported for CW orgs participating in TEFCA
T-HCO-CC	Care Coordination / Case Management	Code supported for CW orgs participating in TEFCA
T-HCO-HED	HEDIS Reporting	Code supported for CW orgs participating in TEFCA
T-HCO-QM	Quality Measure Reporting	Code supported for CW orgs participating in TEFCA

A.4 Network Codes

Network codes should be used for any network specific configuration or settings as defined by the API.

Code	Name
CommonWell	CommonWell
Carequality	Carequality
TEFCA	Trusted Exchange Framework and Common Agreement

A.5 Mime Types

The following Mime types are supported.

Mime Type	Note
xml	<Concept displayName="text/xml" codeSystem="N/A" code="text/xml"/>
plain	<Concept displayName="text/plain" codeSystem="N/A" code="text/plain"/>
pd	<Concept displayName="application/pd" codeSystem="N/A" code="application/pd"/>
x-hl7	<Concept displayName="application/x-hl7" codeSystem="N/A" code="application/x-hl7"/>
dicom	<Concept displayName="application/dicom" codeSystem="N/A" code="application/dicom"/>
multipart/related	<Concept displayName="multipart/related" codeSystem="N/A" code="multipart/related"/
tiff	<Concept displayName="image/tiff" codeSystem="N/A" code="image/tiff"/>
jpeg	<Concept displayName="image/jpeg" codeSystem="N/A" code="image/jpeg"/>
gif	<Concept displayName="image/gif" codeSystem="N/A" code="image/gif"/>
pdf	<Concept displayName="application/pdf" codeSystem="N/A" code="application/pdf"/>
png	<Concept displayName="image/PNG" codeSystem="N/A" code="image/PNG"/>

Appendix B – Performance Targets and Timeout Settings

The CommonWell Health Alliance has agreed on standard performance targets for the main categories of services currently provided by CommonWell. Additionally, the CHA Broker has set timeouts for the document query and document retrieve functionality for both the Integration and Production environments.

B.1 Performance Targets

Pilot Performance Targets	CommonWell Service Provider Targets	CommonWell Member Targets
Non bulk-load PIX and CommonWell REST transactions	99% within 1 second	N/A
CHA Broker document retrieve	90% within 10 seconds	90% within 5 seconds
CHA Broker document query	99% within 6 seconds	99% within 3 seconds

B.2 CHA Broker Timeout Settings for Integration and Production

These timeout settings are subject to change based on member feedback and discussion. The timeout settings listed below are accurate as of this writing.

Environment	Document Query Responding Gateway Individual Request Timeout	Document Query Total Timeout (Doc Query + In-band)	Document Retrieve Responding Gateway Individual Request Timeout	Document Retrieve Total Timeout
Integration	40 seconds	50 seconds	60 seconds	100 seconds
Production	40 seconds	50 seconds	60 seconds	100 seconds

References

Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997. (https://www.rfc-editor.org/rfc/rfc5988)

[RFC2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk Nielsen, L. Masinter, P. Leach and T. Berners-Lee, “Hypertext Transfer Protocol — HTTP/1.1,” RFC 2616, June 1999. This RFC obsoletes RFC 2068. (http://www.ietf.org/rfc/rfc2616.txt)

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” STD 66, RFC 3986, January 2005. (http://www.ietf.org/rfc/rfc3986.txt)

[RFC4627] Crockford, D., “The application/json Media Type for JavaScript Object Notation (JSON),” RFC 4627, July 2006. (http://www.ietf.org/rfc/rfc4627.txt)

[RFC5988] Nottingham, M., “Web Linking,” RFC 5988, October 2010. (http://tools.ietf.org/html/rfc5988)

[RFC6906] Wilde, E., “The ‘profile’ Link Relation Type,” Informational, RFC 6906, March 2013. (http://www.rfc-editor.org/rfc/rfc6906.txt)

[ECMA] European Computer Manufacturers Association, “ECMAScript Language Specification 3rd Edition,” December 1999. (https://www.ecma-international.org/publications- and-standards/standards/ecma-262/)

[ITI TF-1] “IHE IT Infrastructure Technical Framework, Volume 1 (ITI TF-1): Integration Profiles,” IHE International, Inc., August 2012. (https://profiles.ihe.net/ITI/TF/Volume1/index.html)

[ITI TF-2a] “IHE IT Infrastructure Technical Framework, Volume 2a (ITI TF-2a): Transactions Part A,” IHE International, Inc., August 2012. (https://profiles.ihe.net/ITI/TF/Volume2/index.html)

[ITI TF-2b] “IHE IT Infrastructure Technical Framework, Volume 2b (ITI TF-2b): Transactions Part B,” IHE International, Inc., August 2012. (https://profiles.ihe.net/ITI/TF/Volume2/index.html)

Informative References

[FHIR] Grieve, G., et al, “Fast Healthcare Interoperability Resources,” HL7, updated May 2013. (http://www.hl7.org/implement/standards/fhir/index.htm)

[HAL] Kelley, M., “JSON Hypertext Application Language,” draft-kelly-json-hal-05, February 2013. (https://tools.ietf.org/id/draft-kelly-json-hal-05.html)

[HIE] Witting, K. and Moehrke, J., “Health Information Exchange: Enabling Document Sharing Using IHE Profiles,” IHE International, Inc., January 2012. (http://www.ihe.net/Technical_Framework/upload/IHE_ITI_White-Paper_Enabling-doc- sharing-through-IHE-Profiles_Rev1-0_2012-01-24.pdf)

[JWT] Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” draft-ietf-oauth- json-web-token-08, May 2013. (http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-08)

[Markle] Estrin, V., Malek, L., and D. McGraw, “The Common Framework: Overview and Principles,” The Markle Foundation, 2006. (https://markle.org/health/markle-common- framework/connecting-professionals/)

Acknowledgements

This document was prepared with the assistance of Frank Frederick, Steven Roth and Boban Jose. Chris Straight, Jeff Sum, Robert Cruz, George Cole, Yvan Charpentier, Tone Sutherland, Rob Wilmot, Jitin Asnaani, Arien Malec, and Dr. David McCallie provided feedback and helpful review comments.