Optum Salt Lake County Interoperability APIs

Developer-friendly, standards-based APIs that enable third party applications for vendors to connect their applications or programs to access Optum Salt Lake County data.

Overview

Optum Salt Lake County Interoperability APIs enable Salt Lake County members to consent to have their data shared with third-party applications. It also allows third-party application owners to connect to provider directories, further referred to as "public non-member specific data."

Optum Salt Lake County Interoperability APIs provide the functionality listed below:

- Enable developers to register member-facing applications

- Enable members to provide consent for an application to access their data

- Use the **HL7 Fast Healthcare Interoperability Resources (FHIR)** standard for member data

- Use the **OAuth 2.0 / Open ID Connect** standard for member authorization

- Use the **HL7 FHIR** standard for sharing public non-member specific data

Release notes

- Reference: FHIRLayerEXchange_ReleaseNotes_OBH_SLC_v1.12_FINAL.pdf

Authorization

To use the Optum Salt Lake County Interoperability API OAuth 2.0 a developer must register their application. An organization must register as a user by creating a One Healthcare ID and complete the registration application through the "App Owner" section of the Vendor Portal before the ability to register applications is accessible.

A registered application is given a client ID and a client secret. The secret should only be used if it can be kept confidential, such as communication between your server and the respective Optum Salt Lake County Interoperability APIs. For insecure implementations, such as mobile apps, PKCE (Proof Key for Code Exchange) is available.

API permissions and scopes

Access tokens have scopes, which define permissions and the resources that the token can access. Scopes are primarily utilized to determine the type of data an application is requesting. Scopes must be explicitly declared; wildcards are not supported. In the current release the following **scopes** are available for the following types of requests:

Note: Any Scope not currently listed is not supported

Patient access

```
patient/Patient.read
patient/ExplanationOfBenefit.read
patient/Coverage.read
```

Public access (not all available in current release)

Provider Directory

```
public/Practitioner.read
public/PractitionerRole.read
public/Organization.read
public/OrganizationAffiliation.read
public/Network.read
public/Location.read
public/HealthcareService.read
```

This gives access to the correct **FHIR** Endpoints.

Our OAuth2 authentication screen requires members consent to share different types of data. **Your application will need to handle the return of a HTTP status codes** from the endpoints if there are authentication or configuration failures.

If the member declines to share information that your application needs, you may display a message explaining why that information is needed and request re-authorization or handle the collection of that information elsewhere within your application.

The default selection will be to share the scopes included in the initial request with your application. If a member declines a scope but later decides they want to change that selection, they'll need to re-authenticate and make a different choice from the OAuth2 screen.

It is important to explain to members why you need certain data

If information limited by a scope is required for your application to properly function and it is not possible to get the information in another endpoint, we recommend providing an explanation about why certain data is needed in your user flow. For example, if you use demographic information to help members autofill tedious data-entry, you might want to explain that benefit before they reach the authorization screen. **It is essential, however, that you give members the full picture.** If they do share data with your application, they should know how long you keep it and if it is used for any other purposes.

Multiple environments are available under Optum Salt Lake County

Use this table to populate the [environment] annotations in any URL below.

Environment [id]	Description
saltlake	Salt Lake County (Production Environment)
sandbox	Sandbox (Testing Environment)

Native mobile application support

For public clients, such as native mobile application OAuth 2.0, supports the **PKCE** extension and enables custom URIs as redirects.

The implementation of the **PKCE** specification enables developers to build mobile applications without requiring a proxy server to route redirect calls to their mobile app.

The **PKCE** extension provides a technique for public clients to mitigate the threat of a "man-in-the-middle" attack. This involves creating a "secret" that is used when exchanging the authorization code to obtain an access token.

PKCE uses a code challenge that is derived from a code-verifier. Optum Salt Lake County Interoperability API 2.0 supports the "S256" style code challenge.

Where the:

code_verifier = random, non-guessable code

code_challenge = BASE64URL-ENCODE(SHA256(ASCII(codeverifier)))

The following additional parameters and values are sent as part of the OAuth2.0 Authorization Request:

- code_challenge
- codechallengemethod = "S256"

URI protocol

The redirect_uri supports any URI protocol. See examples below:

- https:// protocol
- custom_uri:// protocol

The https:// format is used for secure communication and is required for all applications in the production environment unless the application is using the Mobile OAuth method for handling callbacks.

custom_uri:// protocol

The custom_uri protocol is used by mobile applications to handle communications directly with your application on a mobile device.

If you are using Mobile OAuth support for communication directly with a mobile device the custom_uri should follow this format:

Top-level.domain(TLD).domain-name[.sub-domain][.app_name]

For example, if the Optum Salt Lake County Interoperability API team created an application we might create a custom_uri of:

api.obh.com

This would then be incorporated into a redirect URI entry. Here is an example:

api.uhc.com&state=8e896a59f0744a8e93bf2f1f13230be5

The following query parameters are required:

Response_type	Code
client_id	Provided upon client application approval.
scope	Space separated list of requested scopes. • Patient access scopes • Public access scopes
state	A random string generated by the client which will be sent back from AuthZ to verify authenticity.
redirect_uri	The URI that the OAuth code request returns the user to.
code_challenge	Client generated random string that is SHA256 hashed and then BASE64 encoded. (See info box below)
code_challenge_method	S256

Code challenge generation

- **Create a random string to use as the code_verifier:**
  eae64b84b53f479d92ab81dce7c8bbe608492951def502d84b4f0cd7
- **Create the SHA256 hash, then base64-URL-encode the string:**
  hI2vVv0Er_dHX9lUJo2O8lbFzkxfChVyM2WcHfODLnU
- **Use the base64 url-encoded string as the code_challenge parameter value.**
- code_challenge_method will always be S256 and each code request must contain a unique code_challenge value.

Example GET Request

GET /oauth/authorize HTTP/1.1

Host: https://authz.[environment].flexobh.optum.com

response_type=code&**client_id**=CLIENT_ID&**redirect_uri**=REDIRECT_URI&**scope**=patient/Patient.read
%20patient/ExplanationOfBenefit.read&state=1234zyx&**code_challenge**=CODE_CHALLENGE&**code_ch
allenge_method**=S256

Upon reaching the payer endpoint, the member will be redirected to the respective OAuth2/OIDC
Identity Provider (IdP) for their plan.

The member will authenticate with the IdP and will eventually be redirected back to the endpoint provided in the authorization request's redirect_uri parameter. When the member arrives back to the redirect_uri, the request will contain the following query string parameters:

- code
- state

Compare the state value to the value sent in the initial token request. The values must match or it is an indication of a potential hijack attempt.

The code value will be exchanged for an authorization token by the client application in a background POST request to the AuthZ token endpoint: https://authz.[environment].flexobh.optum.com/oauth/token

The following POST parameters will be sent:

Parameter name	Parameter value
grant_type	authorization_code
code	The code returned in the redirect.
redirect_uri	The same redirect URI sent in the code request.
client_id	The client secret provided during application approval. -OR-
code_verifier	The original random string that was used for the code_challenge parameter in the code request. Do not SHA256 hash it or base64 encode it.

Sample token request

POST /oauth/token HTTP/1.1

Host: https://authz.[environment].flexobh.optum.com

Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&**code**=AUTH_CODE_HERE&**redirect_uri**=REDIRECT_URI&**client_id**=CLIENT_ID&client_secret=CLIENT_SECRET&**code_verifier**=CODE_VERIFIER

(choose either client_secret or code_verifier)

The POST response will return a JSON object with the following properties:

access_token	The access token used for data requests.
refresh_token	Used to request new access tokens.
expires_in	The expiration time of the access token.
scope	The scope values the token supports.
patient	The patient identifier used for FHIR requests

Sample token response

```
{
"access_token": "RsT5OjbzRn430zqMLgV3Ia",
"patient": "2234234234"
"expires_in": 3600,
"scope": "patient/patient.read",
"refresh_token": "PiV5OjbzRn520zwCJwV3Ia"
}
```

Client credentials (system-to-system) and Public access

For system-to-system and public access authentication, the token endpoint supports the client_credentials grant. In this case, the token endpoint is requested, and a token response will be received.

POST /oauth/token HTTP/1.1

Host: https://authz.[environment].flexobh.optum.com

grant_type=client_credentials&**client_id**=CLIENT_ID&**client_secret**=CLIENT_SECRET&**scope**=public/Practitioner.read%20user/PractitionerRole.read

Refresh tokens

The access token will be short-lived, typically 5 minutes or less.

If the data request returns an HTTP 400 response, the access token has likely expired, and the refresh token must be utilized to receive a new access token.

To receive a new access token, a **POST** request to the above token endpoint with the grant_type=refresh_token and refresh_token= will return a token response with a new access token. A new refresh token will not be issued.

Refresh POST example:

POST /oauth/token HTTP/1.1

Host: https://authz.[environment].flexobh.optum.com

grant_type=refresh_token&**refresh_token**=xxxxxxxxxx&client_id=CLIENT_ID&client_secret=CLIENT_SECRET

Refresh tokens must be secured. A refresh token is long-lived and may be used to issue access tokens that provide access to a member's information for the duration of the refresh token's lifetime.

Using access tokens

Resource requests to the FLEX layer require an OAuth2 authorization token provided in the HTTP Authorization header in the format if the example below:

Example request
curl -H "Authorization: Bearer AeT4OkbzMr288gJ2ag9Fwe"
https://fhir.[environment].flexobh.optum.com/R4/ExplanationOfBenefit

Core resources

Base request URL

https://fhir.[environment].flexobh.optum.com/R4

Metadata capability statement

https://fhir.[environment].flexobh.optum.com/R4/metadata

Well known configuration URL

https://fhir.[environment].flex.optum.com/R4/.well-known/smart-configuration

Non-member specific (not all available in current release)

Healthcare Service [PDEX Plan net] (not available in current release)

The Healthcare Service resource typically describes services offered by an organization/practitioner at a location. The resource may be used to encompass a variety of services covering the entire healthcare spectrum, including promotion, prevention, diagnostics, pharmacy, hospital and ambulatory care, home care, long-term care, and other health-related and community services.

Method (read):

GET [base]/HealthcareService/[id]

Method (vread):

GET [base]/HealthcareService/[id]/_history/[vid]

Method (search):

GET [base]/HealthcareService?service-category=prov

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
name	string
organization	reference (organization)
service-category	token
specialty	token

Examples:

GET [base]/HealthcareService?service-category=prov&name=Stewart

GET [base]/HealthcareService?service-category=prov&name=Stewart&specialty=207R00000X

Location [PDEX Plan net] (not available in current release)

A Location is the physical place where healthcare services are provided, practitioners are employed, organizations are based, etc.

Locations can range in scope from a room in a building to a geographic region/area.

Method (read):

GET [base]/Location/[id]

Method (vread):

GET [base]/Location/[id]/_history/[vid]

Method (search):

GET [base]/Location?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
address	string
address-city	string
address-postalcode	string
address-state	string

Examples:

GET [base]/Location?address=Orlando

GET [base]/Location?address-state=CA

GET [base]/Location?address-postalcode=97035-2591

Organization [PDEX Plan net]

An organization is a formal or informal grouping of people or organizations with a common purpose, such as a company, institution, corporation, community group, or healthcare practice.

Method (read):

GET [base]/Organization/[id]

Method (vread):

GET [base]/Organization/[id]/_history/[vid]

Method (search):

GET [base]/Organization?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
address	string
name	string

Examples:

GET[base]/Organization?name=Utah Hospital

Network [PDEX Plan net] (not available in current release)

A network is a type of organization search using the profile parameter.

Method (search):

GET [base]/Organization?type=ntwk

Search parameters: see Organization

Note: Any search parameter not listed is not supported

Name	Type
[Organization searchParameter]	ntwk

Example:

GET [base]/Organization?type=ntwk

Organization Affiliation [PDEX Plan net] (not available in current release)

The Organization Affiliation resource describes relationships between two or more organizations, including the services one organization provides another, the location(s) where they provide services, the availability of those services, electronic endpoints, and other relevant information.

Method (read):

GET [base]/ OrganizationAffiliation/[id]

Method (vread):

GET [base]/OrganizationAffiliation/[id]/_history/[vid]

Method (search):

GET [base]/OrganizationAffiliation?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
network	reference (organization)
participating-organization	reference (organization)
primary-organization	reference (organization)

specialty	token

Examples:

GET [base]/OrganizationAffiliation?specialty=230000000X

Practitioner [PDEX Plannet]

Practitioner is a person who is directly or indirectly involved in the provisioning of healthcare.

Method (read):

GET [base]/Practitioner/[id]

Method (vread):

GET [base]/Practitioner/[id]/_history/[vid]

Method (search):

GET [base]/Practitioner?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
family	string
given	string
name	string

Examples:

GET [base]/Practitioner?name=Smith

GET [base]/Practitioner?given=Scott

Practitioner Role [PDEX Plan net] (not available in current release)

Practitioner Role describes details about a provider, which can be a practitioner or an organization. When the provider is a practitioner, there may be a relationship to an organization.

A provider renders services to patients at a location. When the provider is a practitioner, there may also be a relationship to an organization. Practitioner participation in healthcare provider insurance networks may be direct or through their role at an organization.

Method (read):

GET [base]/PractitionerRole/[id]

Method (vread):

GET [base]/PractitionerRole/[id]/_history/[vid]

Method (search):

GET [base]/PractitionerRole?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
network	string

organization	string
practitioner	string
role (code)	string
specialty	string

Examples:

GET [base]/PractitionerRole?specialty=340000000X

GET [base]/PractitionerRole?location.address-state=ID

Member specific

Patient [CARIN BB]

Demographics and other administrative information about an individual or animal receiving care or other health-related services. Optum Salt Lake County supports versioned reference resources.

Method (read):

GET [base]/Patient/[id]

Method (vread):

GET [base]/Patient/[id]/_history/[vid]

Method (search):

GET [base]/Patient?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string

| _id | string |

Coverage [CARIN BB]

This resource provides the coverage data that was effective as of the date of service of the claim. Optum Salt Lake County supports versioned reference resources.

Method (read):

GET [base]/Coverage/[id]

Method (vread)

GET [base]/Coverage/[id]/_history/[vid]

Method (search):

GET [base]/Coverage?_id=[id]

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string

Explanation of Benefit [CARIN BB]

This resource provides: the claim details; adjudication details from the processing of a Claim; and optionally account balance information, for informing the subscriber of the benefits provided. Optum Salt Lake County supports versioned reference resources.

No records dated prior to 2016-01-01 will be returned.

Method (read):

GET [base]/ExplanationOfBenefit/[id]

Method (vread)

GET [base]/ExplanationOfBenefit /[id]/_history/[vid]

Method (search):

GET [base]/ExplanationOfBenefit?patient=[id] -patient is a required parameter

Search parameters:

Note: Any search parameter not listed is not supported

Name	Type
_count	string
_getpagesoffset	string
_id	string
_lastUpdated	date
identifier	token
patient	string
service-date	date range
type	string

Examples:

GET [base]/ExplanationOfBenefit/219

GET [base]/ExplanationOfBenefit?patient=[id]&_lastUpdated=gt2019

GET [base]/ExplanationOfBenefit?patient=[id]&type=|oral

Production API access

The process for registering production applications mimic our sandbox process above. It is highly recommended that you first register your application as a Sandbox application. Doing so will result in

immediate access to mock data to test your application. Once your testing is complete, then you will need to re-register your application as a Production application.

Production application for use with Public Access API (Provider Directory) will be automatically approved. Production application requests for Patient Access APIs will require review from our security and compliance team prior to approving access. Our security and compliance team will reach out with any questions during this review process.

Patient access authentication launch URLs

Approved production applications that will be used to access member data will need to support 4 separate launch URLs. Optum Salt Lake County's Interoperability APIs requires member authentication via the IdP (identity provider), One Healthcare ID, prior to authorization.

Developer guidelines

Below are guidelines you should follow to be successful in your Optum Salt Lake County Interoperability API integration.

Your privacy policy

You will be asked to provide a URL to your privacy policy when registering your organization and your application in the Optum Salt Lake County Interoperability App Owner Portal. These links should be easy to access and understand by a member using your app.

Member revokes access

A member may revoke access to your application via their member portal. When you encounter an invalid token indicating a member has revoked access, you should make a reasonable attempt to handle that case making it easy for the member to understand what is happening with their data.

Join the developer sandbox

To join the developer sandbox, register a sample application and retrieve synthetic data for a sample Patient ID by calling the API, follow these four steps:

Note: Only Google Chrome and mobile browsers are supported at this time

Step 1: Register a sample application by navigating to the Optum Salt Lake County Interoperability API landing page and clicking the App Owner tile.

App Owner

Registration portal for vendors to register applications to access members data
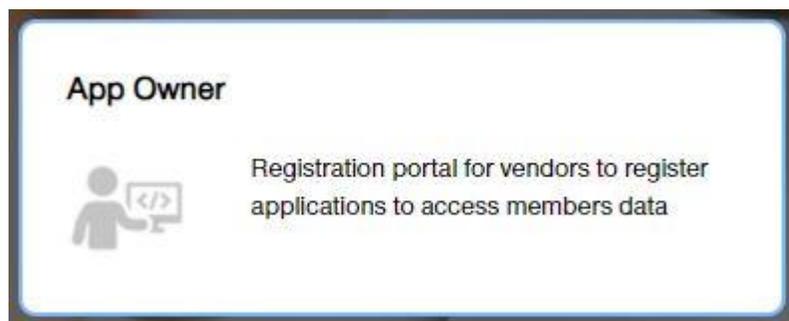
Screen shot of landing page below:

Step 2: Create a One Healthcare ID. All users must create a One Healthcare ID to access the App Owner portal.

Step 3: Create your profile (Note: you will only see this page once at initial login.)

Step 4: Register your organization (Note: This is a one-time process. On your next login you will default to a dashboard view of all applications).

Our security and compliance team will review your organization registration and approve or deny your ability to register applications.

Organization Registration

* All Questions are mandatory

Organization Demographics

List the name of your company *

What is the primary Mailing address of the organization offering this app? *

What is the Federal Tax ID Number or Business Identifier for this Organization *

What is the Physical address of the organization offering this app? *

○ US Number   ○ International Number

Privacy and Security

Have any of the named officers been convicted of felonies in the U.S. or been sanctioned by a governmental agency in the past three years? *

Select ⌄

Do you maintain a Privacy Policy that is shared with your application users? *

Select ⌄

Are any business offices located in any of the following regions - China, Russia, Iran, North Korea ? *

Step 5: Upon approval you will be able to log back into the App owner portal and begin registering applications.

Step 6: "Register New App" to register new application and choose sandbox as the environment (Note: Sandbox is only applicable for Patient Access apps or apps using both Patient access and Public access APIs).

Step 6.1: Obtain Client ID and Secret.

Authentication and authorization

URL - **https://sandbox.authz.saltlake.flexobh.optum.com/**

Base URL for Sandbox API calls https://sandbox.fhir.saltlake.flexobh.optum.com/R4

To test out your sandbox application with the Optum Salt Lake County Interoperability API, you will need to create a test member account via One Healthcare ID when prompted to login as part of the authentication/authorization process. Note: You can use the same One Healthcare ID that was registered to access the vendor portal and register applications.

Support and Registration Information

Optum Salt Lake County will offer the following support consistent with stated government regulations and current operational guidelines.

General support hours

General support hours are available Monday through Friday from 9:00 am to 4:00 pm CST. General support is not provided on holidays or weekends. General support hours apply to:

- Vendor registration (organization or application)
- The developer sandbox environment

System monitoring

Optum Salt Lake County regularly monitors system operations and responsiveness. The system is expected to be operational 24 hours a day, 7 days a week and 365 days a year. System functionality support is available 24 hours a day, 7 days a week and 365 days a year for:

- Vendor API Call Receipts and Responses (Support Available every day)

Registration and response times

The system will accept and respond to organizational and application registration submissions from third party application vendors as follows:

Registration type	Estimated response time[1]
New Organization Registration	5 business days
New Application Registration (Public Access)	No approval required
New Application Registration (Patient Access)	5 business days
Determination Appeals	5 business days from receipt of request

Support request response times

Support request	Estimated response time[1]
Developer Sandbox Support Request	48 business hours

Vendor Production Support Request	24 business hours

Data	Data feed timeframe
Claims	1 business day from adjudication
Encounter data	1 business day from receipt of encounter
Clinical data	1 business day from receipt of data
Provider directory	30 calendar days of a payer receiving provider directory information OR an update to provider directory information

Contact Us

For any question or concerns regarding registering your organization or application please contact **flexvendorsupport@optum.com**.

Back to Top

Disclaimers

1. Response times do not include holidays or weekends.
2. Longer timeframes may be expected in the case of a large-scale systemwide outage.