
# Technical Documentation for Third-party Application Developers

# Table of Contents

# Overview

The Lasso Healthcare Patient Access Application Program Interface ("API") allows third-party application developers to register their third-party applications, allowing Lasso Healthcare members the ability to easily access their health information, such as claims and encounter information (including provider remittances and enrollee cost-sharing). Lasso Healthcare's Patient Access API is based on Health Level 7 Fast Healthcare Interoperability Resources (FHIR) standards for member data and OAuth 2.0 / Open ID Connect standards for member authorization.

Several resources are available on this page to help third-party application developers in creating applications. Information is also available on how to register and get a third-party application authorized with Lasso Healthcare and how to connect an application to the Lasso Healthcare FHIR server.

# Application Registration

Lasso Healthcare requests that third-party applications who wish to connect to Lasso Healthcare's Patient Access API complete a registration process. To register, contact Lasso Healthcare at interoperability@lassohealthcare.com. Our team will request specific information about your organization and application at that time. Please be prepared to provide the name of your application and a callback URI to assign to your application, which will be used during the authorization flow.

After you register your application, you will be given a client ID and a client secret which you will need during authentication. The secret should only be used if it can be kept confidential, such as communication between your server and the Lasso Healthcare Patient Access API.

Note: if you fail to store your application's client ID and client secret, you will have to restart the application registration process.

# Authorization

## *Overview*

Lasso Healthcare's Patient Access API enables Lasso Healthcare members to consent to have their data shared with third-party applications, including their claims and encounter information (including provider remittances and enrollee cost-sharing).

Lasso Healthcare's Patient Access API provides the following functionality:

- Enable members to provide consent for a third-party application to access their health information
- Use the HL7 Fast Healthcare Interoperability Resources (FHIR) standard for member data
- Use the OAuth 2.0 / Open ID Connect standard for member authentication and authorization
- Use of the SMART App Launch with SMART authorization and resource retrieval authorization sequence

## *Access Token Flow*

After sending an authorization request, the Lasso Healthcare member will be directed to a Lasso Healthcare login page through browser re-directs, where they will provide their Lasso Healthcare credentials to authenticate themselves. Upon login, the member will be presented with a consent page. Once the member consents to share their data with your application, your application can exchange the code provided in the redirected request for a full token to make calls to the Lasso Healthcare FHIR server.

Example GET request:

https://lhc-interop-prod-authproxy.azurewebsites.net/api/AadSmartOnFhirProxy/authorize?response_type=code&state=sk31jdsjall389…
&client_id=xxx03lsdks0…
&scope=patient/*.read launch/patient fhirUser offline_access
&redirect_uri=https://yourapp.com/oauth/redirect

Upon reaching the payer endpoint, the member will be redirected to the Register/Log In screen for Lasso Healthcare.

The member will authenticate with their Lasso Healthcare credentials 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:

Token request:

https://lhc-interop-prod-authproxy.azurewebsites.net /api/AadSmartOnFhirProxy/token

Request Body:

grant_type: "authorization_code"
code: "eyJraWQiOiJaZnE2aTR0cmU0aEdFd19CNFd2Q2t"
redirect_uri: "https://yourapp.com/oauth2/callback"
client_id: "63580588-254d-9422-b54e-65872d27dq6f"
client_secret: "M-fZ93kGX1A5_m.8C5qaC_Lg4-UFCA8sGu"

Sample token response:


```
{
"access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOi…",
"id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsI…",
"token_type": "Bearer",
"not_before": 1624998269,
"refresh_token": "BGr8wt3344_OQsAOU.AgABAAAAAAD--DLA…",
"expires_in": 3600,
"expires_on": 1625001869,
"id_token_expires_in": 3600,
"profile_info": "eyJ2ZXIiOiIxLjAiLCJ0aWQiOiI2NjQ0NDdhM…",
"scope": "patient/*.read launch/patient offline_access",
"patient": "d3548a07-a4bc-4143-8d7e-52a2a0e649b2"
}
```


Refresh tokens:
The access token will last 3600 seconds (1 hour).

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

To receive a new access token, POST a request to the 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 every time the access token expires.

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.

# API Permissions and Scopes

## *Requested Data*

Access tokens have scopes, which indicate which parts of the user's account you have permission to access. Scopes are primarily used to determine the type of data an application is requesting. Scopes must be explicitly declared. The following scopes are available for the following types of requests:

Note: Any scope not currently listed is not supported.

Patient Access Scopes:

- patient/*.read
- launch/patient
- fhirUser
- offline_access

This gives access to the correct FHIR endpoints.

## *Member Consent to Share Data*

The OAuth2 authorization screen requires members to consent to share their health information with a third-party application. **Your application will need to handle the return of HTTP status**

**codes** from the endpoints if there are authentication or configuration failures. If a member chooses not to share information that your application needs, you may display a message explaining why that information is needed and request re-authorization.

If the user does not affirmatively select “Allow Access” an access token will not be provided.

We recommend explaining to members why certain data is needed in your application’s user flow. If they do share data with your application, they should know how long the data is kept and if it is used for any other purposes.

# Patient Access API Resources

## *URLs*

Base FHIR URL: https://fhir.lassohealthcare.com/fhir/

Metadata URL: https://fhir.lassohealthcare.com/fhir/metadata

Smart On FHIR Well known configuration URL: https://fhir.lassohealthcare.com/fhir/.well-known/smart-configuration

### *HTTP Status Codes*

| HTTP Status Code | Description |
|---|---|
| 200 | Successful Request |
| 400 | Invalid Parameter |
| 401 | Not Authorized |
| 403 | Insufficient Scope |
| 404 | Unknown Resource |
| 410 | Deleted Resource |

### *Search Parameters*

| Search Parameter Types | Parameters for all resources | Search results parameters |
|---|---|---|
| Number | _id | _sort |
| Date/DateTime | _lastUpdated | _count |
| String | _tag | _include |
| Token | _profile | _revinclude |
| Reference | _security | _summary |
| Composite | _text | _total |
| Quantity | _content | _elements |
| URI | _list | _contained |
| Special | _has<br>_type | _containedType |

Fetch and search criteria, along with common and resource-specific search parameters, can be found at https://www.hl7.org/fhir/search.html.

# Testing Process

## *Overview*

Upon registering your organization and application with Lasso Healthcare, testing will be conducted to confirm that configuration was completed correctly. The following functionality will be tested:

- Manual registration of the application with the OAuth 2.0 Service and appropriate filtering of information for a representative sample set of deidentified members and their corresponding data
- Application registration: client ID, client secret, custom information, redirect URI configuration

Lasso Healthcare's Patient Access API requires member authentication through use of their Lasso Healthcare credentials prior to consenting to share their data with a third-party application.

# Privacy and Security Guidelines

## *Access Security and Compliance*

Lasso Healthcare API requests make use of member-specific information which could be exploited by malicious actors resulting in exposure of member data. Therefore, all Lasso Healthcare patient access transactions must be secured appropriately and held to regulation standards. Access will be limited to authorized individuals, data will be protected in transit, and appropriate audit measures will be taken.

## *Privacy Policy*

You will be asked to provide a URL to your organization's privacy policy when registering your organization and application with Lasso Healthcare. These links should be easy to access and understand by a member using the application.

## *Member Ability to Remove Access*

A member may remove access to your application at any time. When you encounter an invalid token, that indicates that a member has removed access and/or your authorized access to that member's information has expired.

# Support and Registration Information

## *General Support*

For questions or concerns regarding registering your organization or application please contact interoperability@lassohealthcare.com.

Lasso Healthcare will reach out to your point of contact regularly to provide system maintenance updates and/or other key notices.

## *System Monitoring*

Lasso Healthcare 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.

## *Registration and Response Times*

Lasso Healthcare will accept and respond to organizational and application registration submissions from third-party applications as follows:

| Registration type | Estimated response time |
|---|---|
| New organization/application registration | 7 days |

| Support request | Estimated response time |
|---|---|
| Third-party production support request | 7 days |

| Data | Data feed timeframe |
|---|---|
| EOB | 1 business day from adjudication |