Patient Access API Specification

2024-05-06

InterSystems Corporation 1 Memorial Drive Cambridge MA 02142 www.intersystems.com

Patient Access API Specification
HealthShare 2024-05-06

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

Patient Access API Specification

1 Patient Access API Overview

Welcome to our Patient Access API, designed in compliance with the CMS 9115-F regulations. This API facilitates secure and efficient access to patient data, utilizing the HL7® FHIR® R4 standard, a globally recognized framework for health care information exchange.

1.1 What is an API?

API stands for "Application Programming Interface" and is a way for an application such as a SMART on FHIR application to interact with a server on the internet. The Patient Access API allows an application, with the member's permission, to access the member's health data. This access allows the application to give a member the ability to view their health data, download a copy of the data, or share the data with other organizations.

2 Connecting Your Application

To connect your application to the Patient Access API, you will need to ensure that your application supports the following standards:

- HL7 FHIR Release 4.0
- OAuth 2.0

2.1 Authentication and Authorization

To secure access to patient (member) data our API employs robust OAuth 2.0 protocols for authentication and authorization. Client applications must already be registered, at which time they receive unique credentials.

To secure access:

1. *Obtain Access Tokens* — Send a request to our authentication endpoint to receive an access token.
2. *Scopes and Permissions* — Access tokens define the scope and level of access, ensuring that applications only access the necessary data.

The Patient Access API makes the member's coverage, explanation of benefits, and all available clinical data available for access by members and their delegates. An API "user" (either the member or their delegate/proxy) accesses their data by using a third-party (client) application that is designed to retrieve and display available information from the Patient Access API. Third-party applications must be given authorization by the user to access the data on the user's behalf. The authentication and authorization mechanism for granting such access to applications is the OAuth 2.0 Authorization Code workflow. The Authorization Code workflow ensures that access is authorized and restricted appropriately as per the regulations governing the Patient Access API.

The following sections provide an overview of the OAuth 2.0 architecture and implementation for the Patient Access API.

2.1.1 Definition of Terms

Resource

A unit of information available in the API — specifically a FHIR resource.

Resource Owner

The user to whom the FHIR resource belongs.

User

A member, or their delegate/proxy, to whom the data belongs and who is responsible for authorizing access to the data.

Delegate/Proxy

A person who has been granted rights to a member's records on the member's behalf. This is commonly the parent or guardian of a child or the adult child of an elderly person, but the rights to authorize access to records may be granted to any person the member chooses.

Resource Server

The FHIR Server that contains the FHIR resources.

Client or Third-Party App

An application, usually mobile or web, that is designed to retrieve FHIR resources from the Resource Server and display them to the user.

Authorization Server

The server that maintains user credentials and where the user logs in to authorize access to the API. The Authorization Server issues authorization codes and tokens to the client applications. The Authorization Server is also known as the "Issuer".

Authorization Code

A code that is issued to a client app by the Authorization Server once a user has successfully authorized access for the client app.

Access Token (OIDC)

An OAuth 2.0 token issued by the Authorization Server. The access token is an OpenID Connect (OIDC) token containing member information and authorized scopes. Access tokens are short lived, providing access for a small window of time, such as 30 minutes, before expiring.

Refresh Token

An OAuth 2.0 token issued by the Authorization Server which may be used to acquire a new access token on behalf of the user without requiring the user to re-authenticate. Refresh tokens are long lived, allowing the application to continue provided user access without frequent authentication requests.

Client ID/Secret

A client ID is issued to each third-party app and uniquely identifies the app to the Authorization Server. The client Secret is a confidential value which enables the client to authenticate itself as a valid client to the Authorization Server.

Claims

Claims are key/value pairs specified in the Access Token to encode information about the Authorization Server, user, and other authorization details. For example, the “iss”claim indicates the “issuer” and the “exp” claim indicates the “Expiration time” of the token.

Scopes

Scopes are a claim within the Access Token, and consist of a space delimited list of text strings indicating precisely what the user has authorized the application to access on the user's behalf. The standard set of scopes includes things like contact information and user information, however for the Patient Access API, a set of scopes describing FHIR resource types and sensitive data types are included in the authorization code workflow. Scopes are encoded into the Access Token to indicate authorization to access the related data.

2.1.2 Specifications and Standards

The OAuth 2.0 workflow implemented for the patient access API adheres to the following specifications and standards:

OAuth 2.0

The OAuth 2.0 specification describes the authorization code workflow, as well as several other workflows not utilized by the patient access API. https://www.rfc-editor.org/rfc/rfc6749.html

SMART on FHIR

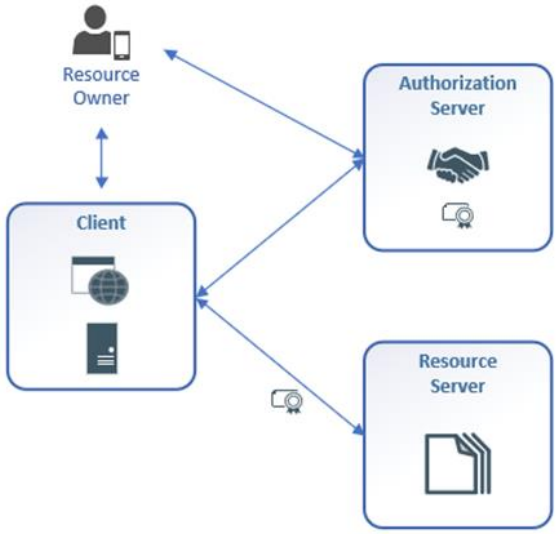
The SMART on FHIR Implementation Guide describes the “SMART App Launch Framework” which specifies how a third-party application should initiate authorization and access to FHIR resources. For the Patient Access API, the specific use case that is implemented is “Patient apps that launch standalone.” http://www.hl7.org/fhir/smart-app-launch/

OpenID Connect (OIDC)

OIDC is an identity layer on top of the OAuth 2.0 protocol which specifies how to encode information about the user and the relevant claims and authorizations the user has made into the Access Token itself. https://openid.net/specs/openid-connect-core-1_0.html

2.1.3 Actors and Configuration

The following actors and configurations enable the OAuth Authorization Code workflow for authorizing access to the Patient Access API:



Resource Owner

The resource owner is the member or proxy that the user has delegated authorization permissions to. The user registers an account with client organization and is issued username and password credentials. The user employs the client application to interact with the Patient Access API.

Client

The client application is the third-party application, typically a mobile application or web site. The client applications that will utilize the Patient Access API will be apps designed to access EOB and clinical information on behalf of the user/member. The apps will be designed to utilize the API metadata and SMART on FHIR configuration file to discover the Authorization Server and initiate the Authorization Code workflow. All client apps must be issued a client ID and Secret by the Authorization Server prior to initiating access to the API.

Authorization Server

The Authorization Server is an OAuth 2.0 Server. It is configured for customization of scopes, and the inclusion of the patient MPIID into the Access Token as required by SMART on FHIR.

Resource Server

The Resource Server is the system that implements the required FHIR Implementation Guides and serves up the coverage, EOB, and clinical information.

The Resource Server validates the Access Token and enforces the scopes that are specified in the token. The Resource Server compares the authorized scopes against the data that is being requested from the API and either allows or disallows the retrieval of the data accordingly.

2.1.4 Patient Identifier API

The OAuth Server is responsible for authorizing members and generating Access Tokens. The OAuth Server includes the patient identifier when responding to client applications. You will need a value for each of the settings below. You should receive these values when you register your application.

Setting	Value Received When You Registered Your Application
API Endpoint	
OAuth Issuer	
Client Name	
Client ID	
OIDC aud	

2.1.5 Endpoints and Operations

The API provides a range of endpoints tailored to various data retrieval needs.

Implementation Guides

The Patient Access API FHIR endpoint is configured using the following implementation guides:

- CARIN Blue Button implementation guide version 1.0.0
- US Core implementation guide version 3.1.1
- DaVinci PDEX implementation guide version 1.0.0
- DaVinci HREX implementation guide version 0.2.0

Profiles and Resources

Profile	Resource
C4BB Coverage	Coverage
C4BB ExplanationOfBenefit Inpatient Institutional	ExplanationOfBenefit
C4BB ExplanationOfBenefit Pharmacy	ExplanationOfBenefit
C4BB ExplanationOfBenefit Professional NonClinician	ExplanationOfBenefit
C4BB Organization	Organization
C4BB Patient	Patient
C4BB Practitioner	Practitioner
US Core AllergyIntollerance	AllergyIntollerance
US Core Condition	Condition
US Core DiagnosticReport-Lab	DiagnosticReport
US Core DiagnosticReport-Note	DiagnosticReport
US Core DocumentReference	DocumentReference
US Core Encounter	Encounter
US Core Immunization	Immunization
US Core ImplantableDevice	Device
US Core ObservationLab	Observation
US Core Location	Location
US Core Medication	Medication

Profile	Resource
FHIR R4 MedicationDispense	MedicationDispense
US Core PractitionerRole	PractitionerRole
US Core Procedure	Procedure
FHIR R4 MedicationStatement	MedicationStatment
FHIR R4 Observation VitalSigns	Observation

3 Compliance and Security

Our API is built with a focus on security and compliance:

CMS 9115-F Compliance

Adherence to CMS 9115-F regulations guarantees the lawful use of patient data.

Data Security Measures

We implement state-of-the-art security measures to protect patient information, ensuring compliance with HIPAA and other privacy laws.

4 Support and Contact Information

Our dedicated Worldwide Response Center (WRC) team is available to assist you with any API-related queries. Contact us at support@intersystems.com.