

Provider Access API Guide



Prepared By:
Acentra Health
1600 Tysons Boulevard, Suite 1000
McLean, VA 22102



evoBrix X v2026-08
September 01, 2026

Table of Contents

Purpose and Scope.....1

Document Conventions 1

Audience Requirements 1

Chapter 1 – Overview 2

 1.1 Data Flow 3

Chapter 2 – Provider Access API.....5

 2.1 Overview 5

 2.1.1 Consent Management.....5

 2.1.2 Operations Involved 6

 2.1.3 Configuration 8

 2.1.4 Provider Access API Documentation.....8

 2.2 FHIR Server Sandbox Environment.....10

 2.3 Accessing the Sandbox Environment 10

 2.4 Base URLs 10

 2.5 Capability Statement 11

 2.6 Resources 11

 2.7 Data Export Search Parameters.....14

 2.8 Request Headers 16

Chapter 3 – Connecting to the Provider Access API 17

Chapter 4 – Third-Party App Registration 18

 4.1 Acentra Sandbox Environment.....18

 4.2 Environments 18

Chapter 5 – Glossary.....19

Chapter 6 – Acronyms 20

Tables

Table 1. Provider Access API Solution Components 2

Table 2. Configuration in Provider Access API..... 8

Table 3: Online Documentation - Provider Access API 8

Table 4. Base URLs for Provider Access API 11

Table 5. Resources and URLs for Provider Access API..... 11

Table 6: Data Export Search Parameters..... 14

Table 7. Request Headers 16

Table 8. Glossary..... 19

Table 9. Acronyms..... 20

Figures

Figure 1: Acentra Interoperability Solution 2

Figure 3. Provider Access API – Data Flow – Payer Systems to FPDR 3

Figure 4. Acentra Sandbox Environment – Online Developer Documentation..... 10

Figure 5. Third-Party App Registration Process 18

Preface

Purpose and Scope

The CMS Interoperability and Prior Authorization Final Rule (CMS 0057 F) released on January 17, 2024 requires CMS-regulated payers to build and maintain a Provider Access API to share patient data with in-network/enrolled providers with whom the patient has a treatment relationship (unless the patient has opted out of having their health information available and shared using the Provider Access API) beginning from January 1, 2026.

This rule has emphasized that the Provider Access API would enable providers to access Claims and encounter data (excluding provider remittances and patient cost-sharing information), USCDI-defined clinical data and Prior Authorization (PA) information and supporting structured documentation (excluding drugs) via Prior Authorization profile.

Also, the rule requires CMS-regulated Payers to establish and maintain an attribution process to associate patients with their in-network or enrolled Providers to enable Payer to Provider data exchange via the Provider Access API.

This document describes Acentra's Interoperability Solution that supports the new CMS mandate.

Document Conventions

This document uses the following conventions:

- The term "you" refers to the application owners who use this document.
- Hyperlink names appear in bold fonts.

Audience Requirements

This document is intended for third-party application owners or developers who need to know how to connect their applications to Acentra's Provider Access API, and for Payers implementing the API to provide data to third-party applications via the API.

Chapter 1 – Overview

The Acentra Interoperability Solution is engineered to support the business and technical requirements defined in the CMS mandate (CMS Final Rule 0057 F). The solution leverages Da Vinci Payer Data Exchange 2.1.0 - STU 2.1 as anchors in conjunction with data exchange standards, such as HL7® Fast Healthcare Interoperability Resources (FHIR®), United States Core Data and Interoperability (USCDI), and CMS recommended Implementation Guides (IGs).

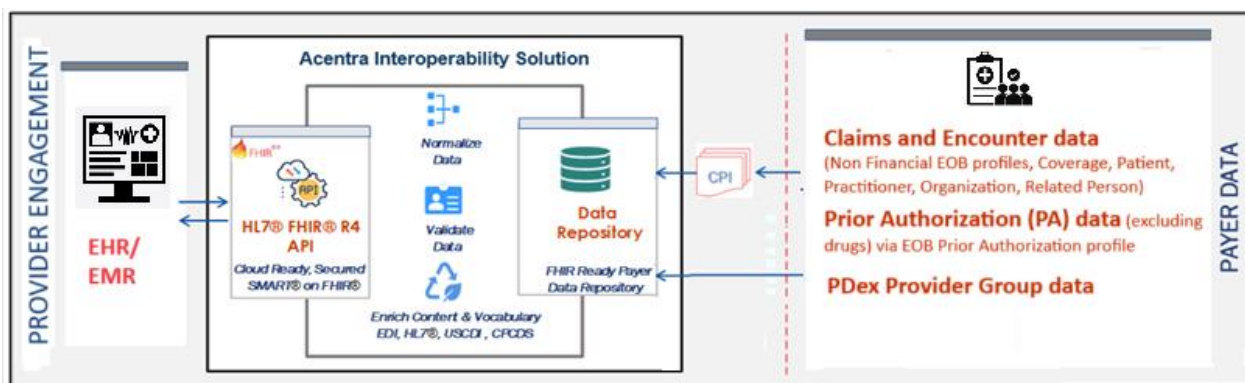


Figure 1: Acentra Interoperability Solution provides a diagram of the overall solution.

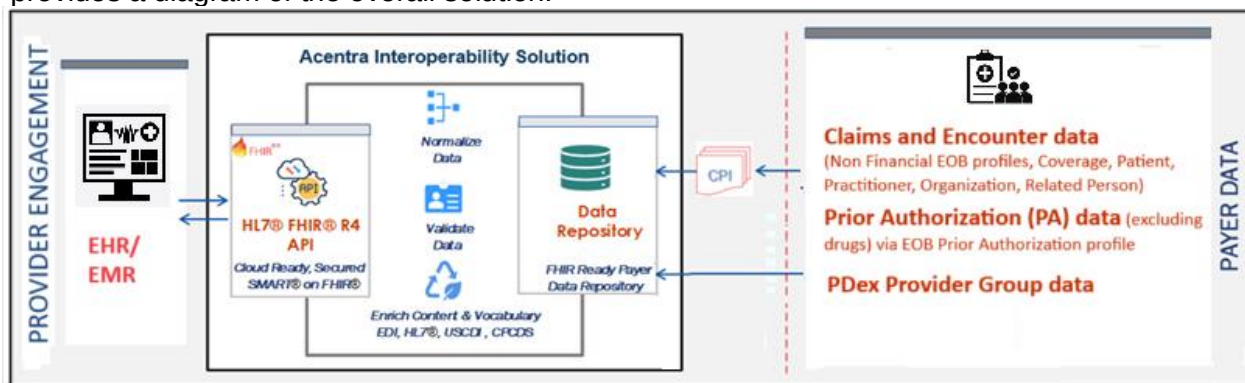


Figure 1: Acentra Interoperability Solution

Table 1 describes the features of the components of the Acentra Interoperability Solution.

Table 1. Provider Access API Solution Components

Component	Features
Mapper	Enables translation of Payer data to a Common Payer Interface (CPI), leveraging pre-built data intake templates. Streamlines the data mapping for Payers by utilizing standardized business attributes with lineage across C4BB profiles, the PDex Prior Authorization profile, PDex Provider Group profile and related frameworks—leveraging industry

Component	Features
	standards to support seamless provider data access. Normalizes and enriches the data before loading to the FHIR Ready Payer Data Repository (FPDR).
Data Repository	FHIR Ready Payer Data Repository (FPDR) integrated with the CPI, enables inter-related models for storing and retrieving data via logical views for Explanation of Benefits (EOBs). Data will be loaded from the Payer Systems on a defined cadence and supplemented with the historical data necessary to meet the data availability requirement. The Provider, Organization, Member and Consent data will be loaded daily, the Claims information will be loaded once every week after the RA Cycle is completed, and the Prior Authorization data will be loaded after Claims.
FHIR Adapter	Facilitates the retrieval of data from FPDR and integrates with the FHIR Server.
FHIR Server	Implements a RESTful FHIR API service that delivers standardized responses based on the CMS-mandated CARIN IG for Blue Button®, Da Vinci PDex Prior Authorization profiles, and PDex Provider Group Profile. The API integrates SMART® on FHIR for secure authentication and authorization, ensuring controlled access for in-network providers to attribute member data.
SMART on FHIR Module	Secures the Provider Access API by implementing the CMS-recommended standalone launch authorization sequence based on the OAuth 2.0 standard. Enables federated authentication with identity providers (IdPs) that support OAuth 2.0 or SAML 2.0, ensuring secure and seamless Provider access to patient data.

1.1 Data Flow

The finalized claims and encounter data (excluding Financial Data), beneficiary demographic data, Coverage data, beneficiary Consent data and Prior Authorization data (excluding drugs) are extracted from the Payer Systems into the pre-defined CPI data intake templates.

The extracted data files will be sent to the Acentra Interoperability Solution using Secure File Transfer Protocol (SFTP) and will be imported into the FHIR-ready Payer Data Repository (FPDR) using the Mapper. Figure 2 depicts a high-level data flow.

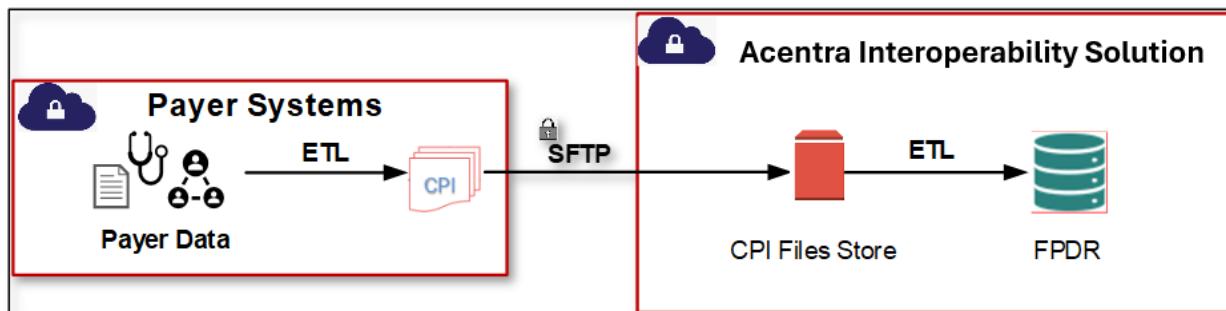


Figure 2. Provider Access API – Data Flow – Payer Systems to FPDR

As part of this process, Acentra's Interoperability Solution normalizes, validates, and enriches the claims and encounter data, beneficiary demographic data, Coverage data, beneficiary Consent data and Prior Authorization data to make it FHIR-ready for third-party apps. The EOB resources combine key information from a claim, a claim response, Prior authorization and provide comprehensive information on the services rendered to a patient by their Provider in accordance with the Patient's coverage terms. Claims will be loaded into the product within a day after they are finalized. Prior Authorization data will be loaded into the product once they are submitted.



The PDex Provider Group Profile does not have a CPI layout. However, the response is populated using data sourced from available CPI layouts, and where data is not present in CPI layouts, it is retrieved directly from the Payer's system.

Chapter 2 – Provider Access API

2.1 Overview

Provider Access API facilitates the secure movement of data from Payer Systems (Producers) to authorized Providers (Consumers) accessible via authorized third-party consumer applications. The Provider Access API leverages the CMS-recommended Da Vinci Payer Data Exchange (PDex) Implementation Guide (IG) and CARIN for Blue Button (C4BB) Implementation Guide (IG) along with the Common Payer Consumer Data Set (CPCDS) as anchors, in conjunction with data exchange standards, such as HL7 FHIR, United States Core Data and Interoperability (USCDI), and SMART on FHIR Application Launch Framework (Standalone Sequence).

Acentra's Interoperability Solution ensures that the data in transit and at rest is encrypted. To ensure authorized access, only the authorized Provider application owners that are approved by the Payer organization will be provided with credentials to initiate a secure connection with FHIR server which is established using TLS 1.2 or higher, ensuring encrypted and authorized communication. In addition, the user connecting with the FHIR server will need to authenticate using the credentials issued by the Payer Organization's Identity Provider. Even after authentication, the SMART on FHIR authorization ensures only the requests carrying a valid OAuth 2.0 access token will be given the appropriate access.

2.1.1 Consent Management

Member must have active or valid consent to enable data exchange with Providers via the Provider Access API. By default, Health Plan members who have not explicitly provided consent information are considered opted-in. Members have the option to opt-out of data sharing via the Provider Access API, as well as to update their preference to revoke a previous denial.

Consent information will be received through the following two sources:

- Consent CPI Layout (or)
- FHIR based API/Web service.

Consent CPI Layout

- Consent information for each Member will be extracted from the Source system through the exclusive Consent Segment 3 (CNS0003) - CPI-MEMBER-PROVIDER-ACCESS-CONSENT-INFO of the Consent CPI Layout.
- Since Members are by default opted in for Provider Access API, if the value for the data element CONSENT-PROVISION-TYPE in the CPI-MEMBER-PROVIDER-ACCESS-CONSENT-INFO segment is null, then the system should consider the Member as opted in for Provider Access Data Exchange and store MEMBER-PROVIDER-CONSENT-STATUS as active in FPDR.
- Any updates to Member consent information must be sent by the Source system through the CPI-CONSENT FILE, which will then be processed and stored in FPDR accordingly.

- When a request is received from a Provider for data exchange through Provider access API, the system will validate the Member's active or valid consent before proceeding with data exchange.
- If the Member does not have active or valid consent, the system must return an appropriate error response during the \$export operation process.

FHIR Webservice

Consent information can also be updated through a FHIR-based API/Web Service, enabling the Payer system to update Member consent information from the Member Portal directly in the FPDR. Members will submit Provider-specific consent information through the Member Portal. The Source system will invoke the FHIR Web service to push the captured consent data to the FPDR.

2.1.2 Operations Involved

The Provider Access workflow enables the FHIR system to establish and maintain Member Groups, validate Provider and Member relationships, determine Member attribution status, and provide authorized access to Member data. The overall functional flow consists of Group Creation, Group Search, Attribution Status, and Bulk Member Export.

1. Group Creation

The FHIR system will create and maintain a Group representing Members and their associated Provider relationships within FPDR.

A Group may be established for Members currently enrolled in the MMIS system (evoBrix X) to define and maintain trusted Member-Provider relationships. Providers registered within the MMIS system and available in FPDR are considered valid Providers for establishing these relationships. Members associated with a Group are considered attributed to the applicable Provider and may be accessed by the Provider through the Provider Access API, subject to applicable validation and consent requirements.

The FHIR system will also support Group creation using a list of Member IDs based on the configuration. A Group creation request may contain one or more existing Member IDs that are to be associated with the newly created Group.



When a group creation request contains 500 member IDs or fewer, the FHIR system shall create the Group synchronously and return the response in the same transaction.

When a group creation request contains more than 500 member IDs, the FHIR system shall create the Group asynchronously.

Since the Member IDs supplied in the request are expected to represent existing Members in the FHIR repository, the system will directly validate and associate the Members with the Group without performing a separate Member Match operation.

The FHIR system supports both synchronous and asynchronous processing of Group creation Request. Upon successful validation and processing, the Group will be created with the applicable Members associated with it.



For group creation requests containing more than 500 member IDs, the request shall include the Prefer: respond-async header to indicate asynchronous processing.

If a request containing more than 500 member IDs is submitted without the Prefer: respond-async header, or attempts to force synchronous processing, the FHIR system shall reject the request and return an appropriate error response:

The submitted bulk FHIR request exceeds the maximum allowed limit. Current limits are 500 resources for synchronous requests and 1500 resources for asynchronous requests. Please reduce the request size and resubmit.

2. Group Search

A Group search request will be performed when a request is received from the Provider, with NPI provided as an input parameter. The FHIR system will validate the request and check if a valid and active Provider record exists in the FPDR. If the Provider is found to be valid and active, the FHIR system will return a Group Search Response to the Provider using the PDex ProviderGroup profile.

3. Attribution Status

The Attribution Status Operation Request will be invoked by a Provider to retrieve the attribution status of a specific Member, using the Group ID and Member ID as input parameters. The system will verify that the Group ID is valid, and that the Member exists in FPDR and is both valid and active. Additionally, the Member must be part of the Group ID provided and must have provided consent for data exchange via the Provider Access API. If all validations are successful, the FHIR system will return a response to the Provider as a Bundle resource that contains Member Attribution List Data for a specific patient through PDex ProviderGroup profile.

4. Bulk Member Export

After the completion of Group search operation request, the Provider invokes the Export operation for a Single Member request using the Group ID and Member ID as input parameters. The system must verify that the Group ID is valid and that the Member is both valid and active in FPDR. Additionally, the Member must have provided consent for data exchange via the Provider Access API. Once the data is processed, the payer's FHIR server should return the Response to the Provider in JSON format containing the requested data.

After the completion of Group search operation request, the Provider invokes the Export operation for Bulk Member request to the Payer's FHIR server using Group ID and multiple Member IDs as input parameters. The system must verify that the Group ID is valid and that each Member is both valid and active in the FPDR. Additionally, each Member must have

provided consent for data exchange via the Provider Access API. The Payer's FHIR server processes the export request, excluding the Member's data who has opted out. Once the data is ready, the Payer's FHIR server should return the response to the Provider in JSON format containing the requested data.

2.1.3 Configuration

Configuration flags have been implemented in Provider access API to perform certain validation checks when the configuration flag is set as "Yes". The System should bypass the validation checks when the configuration flag is set as "No" and directly sends the response data to the requesting Provider.

Table 2 demonstrates the System behavior based on the Configuration in Provider access API.

Table 2. Configuration in Provider Access API

Configuration in Provider Access API	When Configuration Flag is "Yes"	When Configuration Flag is "No"
For including other Payer data into API Response	API Response must include both current Payer data and other Payer (external) data w.r.t the member.	API Response must include only current Payer data w.r.t the member.
Group validation	The System performs all Group validation checks	The System bypasses Group validation and directly sends the response data to the requesting Provider.
Member Consent validation	The System performs all Member Consent validation checks	The System bypasses Member Consent validation and directly sends the response data to the requesting Provider.
Member validation	The System performs all Member validation checks	The System bypasses Member validation and directly sends the response data to the requesting Provider.
File Retrieval Method	The system sends a pre-signed download URL.	The system sends a file retrieval API endpoint.

2.1.4 Provider Access API Documentation

Error! Reference source not found.3 provides links to the online documentation for the Provider Access API.

Table 3: Online Documentation - Provider Access API

Function	Online Documentation
IG References	Provider Access API IG

Function	Online Documentation
	https://build.fhir.org/ig/HL7/davinci-epdx/provider-access-api.html#provider-access-api-1 Bulk Data Access IG https://hl7.org/fhir/uv/bulkdata/index.html#bulk-data-ig-home-page Member Attribution List IG Detailed Specification - Da Vinci - Member Attribution (ATR) List v2.0.0
Claims and Encounters Data	HL7.FHIR.US.CARIN-BB\Artifacts Summary - FHIR v4.0.1 C4BB ExplanationOfBenefit Inpatient Institutional Basis - CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) v2.1.0 C4BB ExplanationOfBenefit Oral Basis - CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) v2.1.0 C4BB ExplanationOfBenefit Outpatient Institutional Basis - CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) v2.1.0 C4BB ExplanationOfBenefit Pharmacy Basis - CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) v2.1.0 C4BB ExplanationOfBenefit Professional NonClinician Basis - CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) v2.1.0
Prior Authorization Data	https://hl7.org/fhir/us/davinci-pdex/STU2/StructureDefinition-pdex-priorauthorization.html#root
Provider Group Data	PDexProviderGroup
Search Parameters	 Provider%20Access%20API-Search%20Par:
Error Codes	 FHIR-Error%20Codes_Provider%20Access%

2.2 FHIR Server Sandbox Environment

Acentra's Interoperability Solution's Sandbox Environment provides a synthetic but reliable dataset for Claims and Encounters to help facilitate testing of the Provider Access API. The Sandbox dataset represents real data and ensures consistency across the dataset.

Detailed information about Acentra's Interoperability Solution Sandbox Environment can be found at <https://sandbox.mhbapp.com/index.html>. The site includes information for contacting Acentra to register your application.

As shown in Figure 3, the Acentra Sandbox FHIR server documentation portal provides all the required information for the third-party app developers to register their app and connect and access the Sandbox FHIR server for Provider Access API.

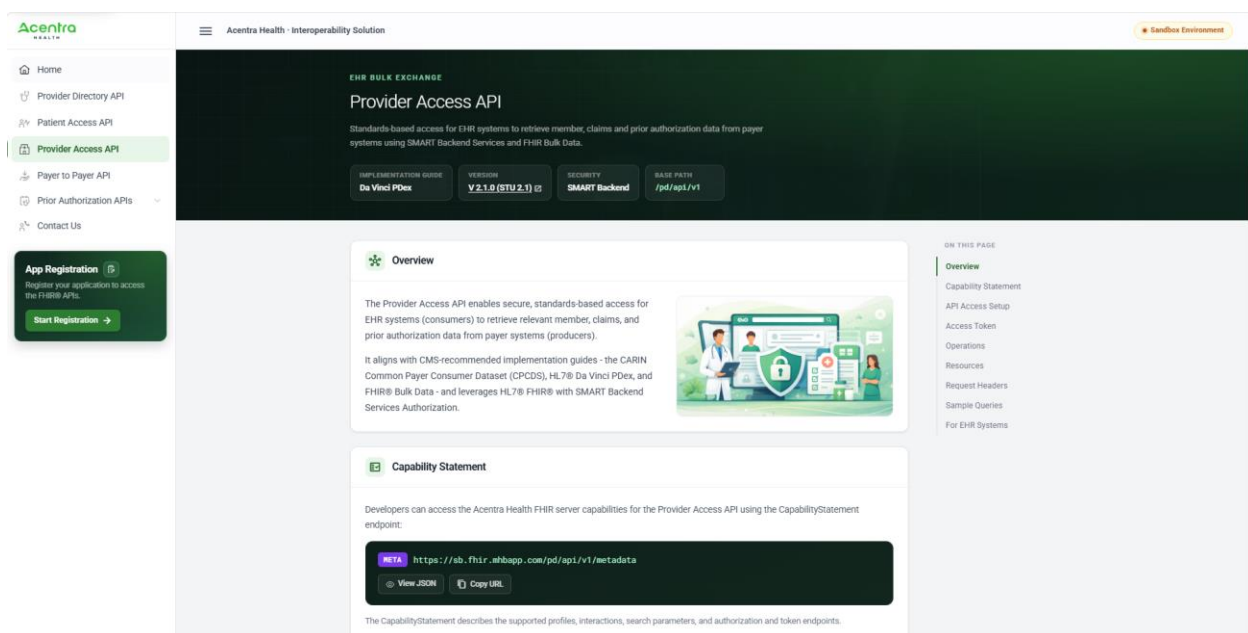


Figure 3. Acentra Sandbox Environment – Online Developer Documentation

2.3 Accessing the Sandbox Environment

Before you can access the Provider Access API, you will need to register your application with Acentra's Sandbox Environment.



Refer to the Sandbox FHIR server documentation information at <https://sandbox.mhbapp.com/index.html>

2.4 Base URLs

Three types of FHIR server URLs are provided below for Provider Access API.

- Acentra Sandbox
- UAT
- Production

Table 4 provides the base URLs for the FHIR server for the Provider Access API. Please note that the base URLs are not accessible via browser and are meant to be accessed programmatically.

Table 4. Base URLs for Provider Access API

Environment	Base URL Provider Access API (<i>base_url_pra</i>)
Acentra Sandbox	https://sb.fhir.mhbapp.com/pd/api/v1/
UAT	<a href="https://<<tenant-id>>.np.fhir.mhbapp.com/pd/api/v1/">https://<<tenant-id>>.np.fhir.mhbapp.com/pd/api/v1/
Production	<a href="https://<<tenant-id>>.fhir.mhbapp.com/pd/api/v1/">https://<<tenant-id>>.fhir.mhbapp.com/pd/api/v1/

2.5 Capability Statement

The capability statement describes the set of capabilities (behaviors) implemented by the FHIR Server; for example, it describes the enabled profiles, interactions, and search parameters and provides information about the authorization and token endpoints.

The FHIR server capabilities for Provider Access API can be accessed using the Capability Statement endpoint: https://<<base_url_pd>>/metadata.

Please refer to Table 4 for the base URLs for Provider Access API. For example - the sandbox environment Capability URL will be: <https://sb.fhir.mhbapp.com/pd/api/v1/metadata>.

2.6 Resources

The Acentra Interoperability Solution's Provider Access API supports the resources listed in Table 5.

Table 5. Resources and URLs for Provider Access API

Resources	URL
Practitioner	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=Practitioner
	https://[baseURL]/Group/[id]/\$davinci-data-export?_type=Practitioner&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=Practitioner
	https://[baseURL]/Group/[id]/\$davinci-data-export?_since=[date]&_typeFilter=Practitioner&patient=[id]

Resources	URL
	https://[baseURL]/Group/[id]/\$davinci-data-export?_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot&_typeFilter=Practitioner&patient=[id]
Patient	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Patient&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_type=Patient&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_since=[date]&_typeFilter=Patient&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot&_typeFilter=Patient&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Patient?_include=Patient:provider&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Patient?_include=Patient:insurer&patient=[id]
Organization	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&typeFilter=Organization
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_type=Organization
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Organization&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Organization&_since=[date]&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Organization&patient=[id]&_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot
	https://[baseURL]/Group/[id]/\$davinci-data-export?_typeFilter=Organization?include=Organization:insurer&patient=[id]
Coverage	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_type=Coverage
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=Coverage
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=2023120&_typeFilter=Coverage&_since=[date]
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=Coverage&_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot

Resources	URL
	https://[baseURL]/Group/[id]/\$davinci-data-export?typeFilter=Coverage?include=Coverage:payor&patient=[id]
RelatedPerson	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=RelatedPerson
	https://[baseURL]/Group/[id]/\$davinci-data-export?type=RelatedPerson&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_since=[date]&_typeFilter=RelatedPerson&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot&_typeFilter=RelatedPerson&patient=[id]
	https://[baseURL]/Group/[id]/\$davinci-data-export?typeFilter=RelatedPerson?_include=RelatedPerson:patient&patient=[id]
Prior Authorization	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[date]&_typeFilter=ExplanationOfBenefit?use=preauthorization
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[date]&_typeFilter=ExplanationOfBenefit?use=preauthorization%26service-date=ge[date]
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?use=preauthorization%26lastUpdated=[date]
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[date]&_typeFilter=ExplanationOfBenefit?use=preauthorization&_since=[date]
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?use=preauthorization&_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?use=preauthorization&_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-download
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?use=preauthorization&_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-delta
ExplanationOfBenefit	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_type=ExplanationOfBenefit
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit

Resources	URL
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_since=[date]&_typeFilter=ExplanationOfBenefit
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_until=[date]&exportType=hl7.fhir.us.davinci-pdex%23provider-snapshot&_typeFilter=ExplanationOfBenefit
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?_include=ExplanationOfBenefit:patient
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?_include=ExplanationOfBenefit:provider
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?_include=ExplanationOfBenefit:insurer
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?_include=ExplanationOfBenefit:care-team
	https://[baseURL]/Group/[id]/\$davinci-data-export?patient=[id]&_typeFilter=ExplanationOfBenefit?_include=ExplanationOfBenefit:coverage

2.7 Data Export Search Parameters

Table 6 provides a list of search parameters that can be used as data export parameters.

Table 6: Data Export Search Parameters

S. No	Parameter	Description	Scenarios
1	patient	To retrieve data for specific members in the Group.	Patient ID to be passed mandatorily with Group ID in input.
2	since	To be used for resource requests when the full history is not required to limit data.	YYYY-MM-DD – Format to be used for input
3	until	Response includes resources updated before the specified time.	YYYY-MM-DD – Format to be used for input

S. No	Parameter	Description	Scenarios
		Mostly used with the <i>hl7.fhir.us.davinci-pdex#provider-snapshot</i> exportType to retrieve member data for a specific period.	
4	_type	This enables providers to only retrieve the resource types they are interested in seeing. Resource types that can be used in this parameter - Patient, Practitioner, ExplanationOfBenefit, Coverage, Organization, RelatedPerson	Example: [base]/Group/[id]/\$davinci-data-export?_type=Patient,Coverage
5	_typeFilter	Specifies a search URL that can be used to narrow the results for one or more of the resource types being exported. When constructing search queries to incorporate into a _typeFilter, Search parameters supported by the relevant profiles from the Pdex or CARIN Blue Button IGs SHALL be followed.	Can be used in conjunction with the _type parameter specifying the elements to limit the resource types as well as to specific search sets within one or more of the resource types. To support multiple typeFilters, separate them by a comma. Examples: [base]/Group/[id]/\$davinci-data-export?_typeFilter=ExplanationOfBenefit?use=preauthorization [base]/Group/[id]/\$davinci-data-export?_typeFilter=Coverage?status=active
6	exportType	The exportType parameter specifies the purpose of the export and SHALL have one of the following values: 1) hl7.fhir.us.davinci-pdex#provider-delta 2) hl7.fhir.us.davinci-pdex#provider-download 3) hl7.fhir.us.davinci-	The hl7.fhir.us.davinci-pdex#provider-delta option SHALL be used when the provider is retrieving new, or updated data that will be stored as part of the patient record. The hl7.fhir.us.davinci-pdex#provider-download option SHALL be used when the provider is retrieving data that will be stored as part of the patient record. The hl7.fhir.us.davinci-pdex#provider-snapshot value SHOULD be used when a

S. No	Parameter	Description	Scenarios
		pdex#provider-snapshot	provider wants to download data for viewing.

2.8 Request Headers

All requests for Provider Access API resources require the headers outlined in Table 7.

Table 7. Request Headers

Headers	Values
content-type	application/json
accept	application/json
authorization	Bearer <<ACCESS_TOKEN>>

Chapter 3 – Connecting to the Provider Access API

- The EHR Client connecting to the FHIR Server must first register as a FHIR-enabled third-party application.
- During registration, the EHR Client must provide its public key in the form of a JSON Web Key (JWK) to enable secure authentication with the FHIR Authorization Server.
- Once registration is successfully completed and approved, the EHR client will be issued a “Client ID” and will be considered pre-authorized to access FHIR resources.
- A secure connection between the EHR Client and the FHIR Server must be established using TLS 1.2 or higher, ensuring encrypted and authorized communication.
- The client must generate a JSON Web Token (JWT) signed using its registered private key. This JWT is used to authenticate the EHR client and will be included in the request for an access token.
- After authentication, the EHR Client must request an access token by sending an HTTP POST request to the FHIR Authorization Server’s token endpoint.
- Upon successful validation, the client obtains an access token via **OAuth 2.0 framework with SMART on FHIR authorization** using asymmetric keys.
- Once authenticated and authorized, the FHIR API endpoint of the Payer system will be known, therefore an EHR Client can:
 - Perform single-member requests to retrieve individual patient data
 - Perform bulk-member requests to retrieve data for multiple patients

Chapter 4 – Third-Party App Registration

4.1 Acentra Sandbox Environment

The Acentra Sandbox Environment is available for third-party app owners to perform connectivity and testing. The third-party app owners can reach out to Acentra directly or via payer organization to register their app. If the payer organization approves the request, then Acentra will provide access. In cases where the third-party app reaches out to Acentra directly, it will be Acentra discretion to approve or deny the request.

4.2 Environments

In the Acentra Interoperability Solution, the intake process collects the registration and attestation information from the third-party app owner and sends it to the authorized personnel from the payer organization (or Tenant). The payer organization uses the information provided by Acentra to conduct third-party app verification.

If approved, the payer organization notifies Acentra and Acentra will issue credentials (client-id) to the third-party app owners for the appropriate environment: Production. If the app registration is not approved, then the payer organization notifies the app owner directly and conveys the decision to Acentra. A graphic of this process is shown in Figure 7.

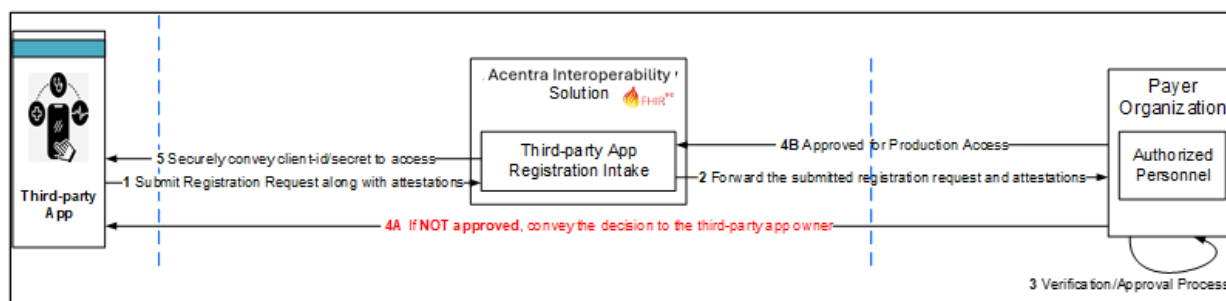


Figure 4. Third-Party App Registration Process

Chapter 5 – Glossary

This section provides definitions for document-specific terms in the following format: Entries are in alphabetical order, and items beginning with numbers will come first.

Table 8. Glossary

Term	Definition
Application Programming Interface	An interface that defines interactions between multiple software applications.
CARIN	A non-partisan, multi-sector alliance focused on providing digital health information to consumers. Also known as CARIN Alliance.
Acentra Interoperability Solution	A solution created to support the business and technical requirements defined in the CMS mandate, CMS Final Rule 0057-F.
Payer Organization	A business entity that adjudicates and renders payment for health care claims, including pharmacy claims. Examples include Medicare, state Medicaid programs, and commercial insurance carriers. In this document, "Tenant" is also used to indicate the Payer Organization in relation to the environment.
Sandbox	An environment containing hardware, instrumentation, simulators, software tools, and other support. Also known as a "test bed".
Tenant	See "Payer Organization".
Third-Party App	An application or program that is neither Acentra nor the Washington State Health Care Authority, that has authorized access via the API for the purpose of delivering data to authorized users (Providers).

Chapter 6 – Acronyms

This section provides definitions for document-specific terms in the following format: Entries are listed in alphabetical order, and items beginning with numbers will come first.

Table 9. Acronyms

Acronym	Definition
API	Application Programming Interface
CMS	Centers for Medicare & Medicaid Services
CPI	Common Payer Interface
EDI	Electronic Data Interchange
EHR	Electronic Health Record.
EOB	Explanation of Benefits
FHIR	Fast Healthcare Interoperability Resources
FPDR	FHIR Ready Payer Data Repository
ID	Identification
IG	Implementation Guide
JWK	JSON Web Key
JWT	JSON Web Token
OIDC	Open ID Connect
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SFTP	Secure File Transfer Protocol
SMART	Substitutable Medical Applications and Reusable Technologies
STU	Standard for Trial Use
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator

Acronym	Definition
USCDI	United States Core Data and Interoperability
PDex	Payer Data Exchange