

Patient Access API Guide



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



evoBrix X v2026-06
July 08, 2026

Table of Contents

Preface.....	1
Purpose and Scope.....	1
Document Conventions	1
Audience Requirements	1
Chapter 1 – Overview	2
1.1 Data Flow	3
Chapter 2 – Patient Access API	5
2.1 Patient Access API Documentation	5
2.2 FHIR Server Sandbox Environment.....	6
2.3 Accessing the Sandbox Environment	6
2.4 Base URLs	6
2.5 Capability Statement	8
1.6 Supported Scopes.....	8
2.7 Authorization URL Format	9
2.8 Getting an Access Token	10
2.9 Resources	10
2.10 Request Headers	11
Chapter 3 – Connecting to the Patient Access API	12
3.1 Identity Provider’s Login Screen	13
3.2 Knowledge-Based Authorization (KBA)	14
3.3 Consent Screen.....	15
Chapter 4 – Third-Party App Registration	17
4.1 Acentra Sandbox Environment	17
4.2 Environments	17
Chapter 5 – Glossary.....	18
Chapter 6 – Acronyms.....	18

Tables

Table 1. Patient Access API Solution Components	2
Table 2. Online Documentation - Patient Access API.....	5
Table 3. Base URLs for Patient Access API.....	7
Table 4. Base URLs for SMART® on FHIR®	8
Table 5. Token Request.....	10
Table 6. Resources.....	10
Table 7. Request Headers	11
Table 8. Glossary.....	18
Table 9. Acronyms.....	18

Figures

Figure 1. Acentra Interoperability Solution	2
Figure 2. Patient Access API – Data Flow – Payer Systems to FPDR	3
Figure 3. Acentra Sandbox Environment – Online Developer Documentation.....	6
Figure 4. Acentra Interoperability Solution – Login Screen (example)	13
Figure 5. KBA Screen (example)	14
Figure 6. Consent Screen	15
Figure 7. Third-Party App Registration Process	17

Preface

Purpose and Scope

On March 9, 2020, the Centers for Medicare and Medicaid Services (CMS) released the Interoperability and Patient Access final rule (CMS-9115-F). To affirm its commitment to advancing interoperability and improving prior authorization processes, it further released CMS Interoperability and Prior Authorization final rule (CMS-0057-F)

This rule requires CMS-regulated payers to make health information easily available to patients by implementing and maintaining a standards-based Application Programming Interface (API) to facilitate the movement of data from payer Systems (Producers) to the patients (Consumers) accessible via third-party consumer apps.

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.
- Italicized portions of the URLs represent placeholders for adding tenant-specific details.
- Screen and hyperlink names appear in bold font.

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 Patient 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 9115-F) and (CMS Final Rule 0057-F). The solution leverages CARIN Common Payer Consumer Dataset (CPCDS) 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), like the CARIN IG for Blue Button® (C4BB) Version 2.0.0 (STU 2 US). Figure 1 provides a diagram of the overall solution.

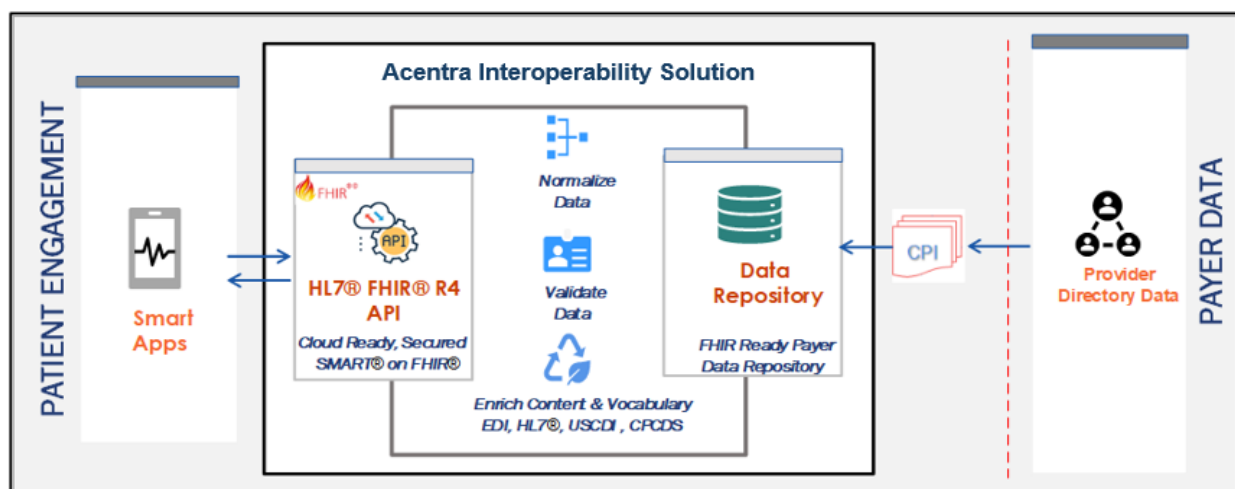


Figure 1. Acentra Interoperability Solution

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

Table 1. Patient 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 using standardized business attributes with lineage across C4BB profiles, PDex Prior Authorization profile, leveraging the CPCDS, HIPAA EDI, and other data standards. 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, and Member data will be loaded daily, the Claims information will be loaded once every week

Component	Features
	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 the REST API service to enable FHIR Standard responses based on CMS-recommended CARIN IG for Blue Button profiles with SMART® on FHIR integration for authentication and authorization.
SMART on FHIR Module	Secures the Patient Access API by implementing the CMS-recommended standalone launch authorization sequence based on the OAuth2 standard. Enables Federated Authentication with a State Identity Provider (IdP) that supports OAuth2 or SAML 2.0.
Knowledge-Based Authorization (KBA) module	Enables the ability to associate the user's Login ID with the Member ID or Patient ID.

1.1 Data Flow

The finalized claims data, beneficiary demographic data and Prior Authorization data 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.

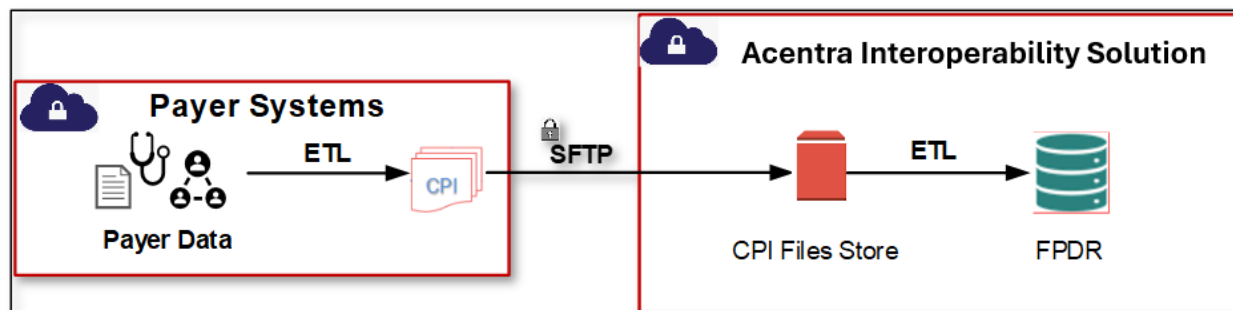


Figure 2. Patient Access API – Data Flow – Payer Systems to FPDR

As part of this process, Acentra's Interoperability Solution normalizes, validates, and enriches the EOB and Prior Authorization data to make it FHIR-ready for third-party apps. The EOB resource combines key information from a claim, a claim response, prior authorization and optional account information to inform a patient of the goods and services rendered by their Provider, and the final payment the Provider received 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.

Chapter 2 – Patient Access API

Patient Access API facilitates the secure movement of data from payer Systems (Producers) to the patients (Consumers) accessible via third-party consumer applications. The Patient Access API leverages the CMS-recommended Da Vinci Payer Data Exchange 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 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 application owners that are approved by the payer organization will be provided with credentials to connect to the FHIR server. 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 with a valid Access Token will be given the appropriate access.

2.1 Patient Access API Documentation

Table 2 provides links to the online documentation for the Patient Access API.

Table 2. Online Documentation - Patient Access API

Function	Online Documentation
Claims and Encounters Data	CARIN IG for Blue Button®
Prior Authorization Data	Da Vinci Payer Data Exchange
Profiles	CARIN IG for Blue Button® Profiles PDex Prior Authorization
Authorization Framework	SMART® on FHIR® Standalone launch Sequence
Search Parameters	 Patient%20Access%20API-Search%20Parai
Error Codes	 FHIR-Error%20Codes_Patient%20Access%2

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 Patient 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 Patient Access API.

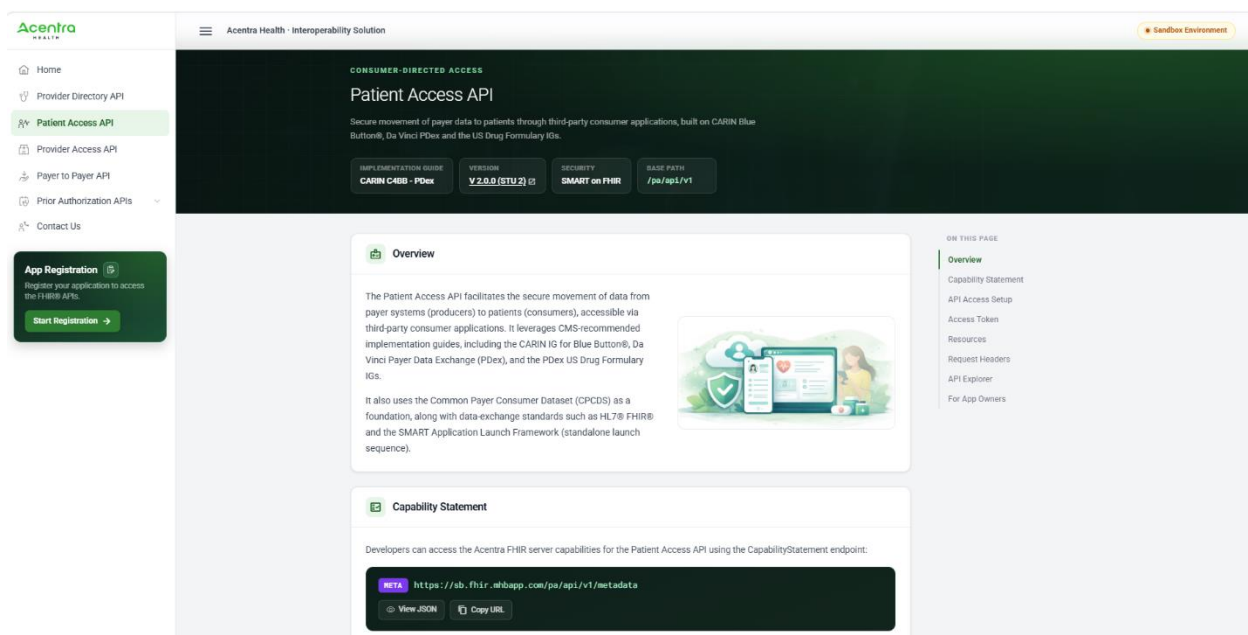


Figure 3. Acentra Sandbox Environment – Online Developer Documentation

2.3 Accessing the Sandbox Environment

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

- Acentra Sandbox
- UAT
- Production

Table 1 provides the base URLs for the FHIR server for the Patient Access API. Please note that the base URLs are not accessible via browser and are meant to be accessed programmatically.

Table 3. Base URLs for Patient Access API

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

Table 1 provides the base URLs for SMART on FHIR. Please note that the base URLs are not accessible via browser and are meant to be accessed programmatically.

Table 4. Base URLs for SMART® on FHIR®

Environment	Base URLs SMART® on FHIR® (base_url_sof)
Acentra Sandbox	https://sb.fhir.mhbapp.com/sof/api/v1/
UAT	<a href="https://<<tenant-id>>.np.fhir.mhbapp.com/sof/api/v1/">https://<<tenant-id>>.np.fhir.mhbapp.com/sof/api/v1/
Production	<a href="https://<<tenant-id>>.fhir.mhbapp.com/sof/api/v1/">https://<<tenant-id>>.fhir.mhbapp.com/sof/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 Patient Access API can be accessed using the Capability Statement endpoint: https://<<base_url_pa>>/metadata.

Please refer to Table 3 for the base URLs for Patient Access API. For example - the sandbox environment Capability URL will be: <https://sb.fhir.mhbapp.com/pa/api/v1/metadata>.

1.6 Supported Scopes

The FHIR Authorization Server supports the following scopes to enable secure access for Patient Access API:

- openid
- fhirUser
- profile
- offline_access
- online_access
- launch/patient
- patient/ExplanationOfBenefit.read
- patient/Coverage.read
- patient/Organization.read
- patient/Patient.read
- patient/Practitioner.read
- patient/RelatedPerson.read
- patient/Provenance.read
- patient/OperationOutcome.read

2.7 Authorization URL Format

The Patient Access API uses the SMART on FHIR standalone launch for authorization and requires "aud", "scope", and "state" in the OAuth2 request as per the specification. Here is an example of a typical authorization URL:

```
https://<<base_url_sof>>/oauth2/authorize?response_type=code&state=123&scope=patient/Patient.read+patient/ExplanationOfBenefit.read+patient/Coverage.read+fhirUser+online_access+user/*.read+openid+profile&aud=https://sb.fhir.mhbapp.com/pa/api/v1&client_id=<<your_client_id>>&redirect_uri={your_redirect_url}
```

2.8 Getting an Access Token

The access token can be obtained by using the Token URL at https://<<base_url_sof>>/oauth2/token. Please refer to Table 4 for the base URLs for SMART® on FHIR®. For example - the sandbox environment token URL will be: <https://sb.fhir.mhbapp.com/sof/api/v1/oauth2/token>.

Table 1 provides the details to be used to submit a token request.

Table 5. Token Request

Request Elements	Required Values	
HTTP Method	Post	
HTTP Headers	Content-type	application/json
	Accept	application/json
	Authorization	Basic base 64 <<you_client_id>>:<<your_client_secret>>
HTTP Body	Code	{oauth code}
	grant_type	"authorization_code"
	redirect_uri	<<your_redirect_uri>>

2.9 Resources

The Acentra Interoperability Solution's Patient Access API supports the resources listed in Table 6.

Table 6. Resources

Resource	URL
/ExplanationOfBenefit	<a href="https://<<base_url_pa>>/ExplanationOfBenefit">https://<<base_url_pa>>/ExplanationOfBenefit
/Patient	<a href="https://<<base_url_pa>>/Patient">https://<<base_url_pa>>/Patient
/Coverage	<a href="https://<<base_url_pa>>/Coverage">https://<<base_url_pa>>/Coverage
/Practitioner	<a href="https://<<base_url_pa>>/Practitioner">https://<<base_url_pa>>/Practitioner
/PractitionerRole	<a href="https://<<base_url_pa>>/PractitionerRole">https://<<base_url_pa>>/PractitionerRole
/Location	<a href="https://<<base_url_pa>>/Location">https://<<base_url_pa>>/Location
/Organization	<a href="https://<<base_url_pa>>/Organization">https://<<base_url_pa>>/Organization

2.10 Request Headers

All requests for Patient 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 Patient Access API

FHIR® interoperability ecosystem users connect to the payer's FHIR® server through the 3rd party application of their choice. Figure 4 below shows the typical authentication, authorization, and patient matching steps to ensure secure and authorized access to a patient's PHI/PII.

- Step#1:** The 3rd party application initiates the SMART® on FHIR® (SoF) compliant 'authorization request' with the FHIR® server
- Step#2:** The FHIR® server federates the user (patient or an authorized caregiver) authentication with the payer's identity provider (IdP) System that supports SAML 2.0 and meets the federal government's technical and policy controls for privacy and information security.

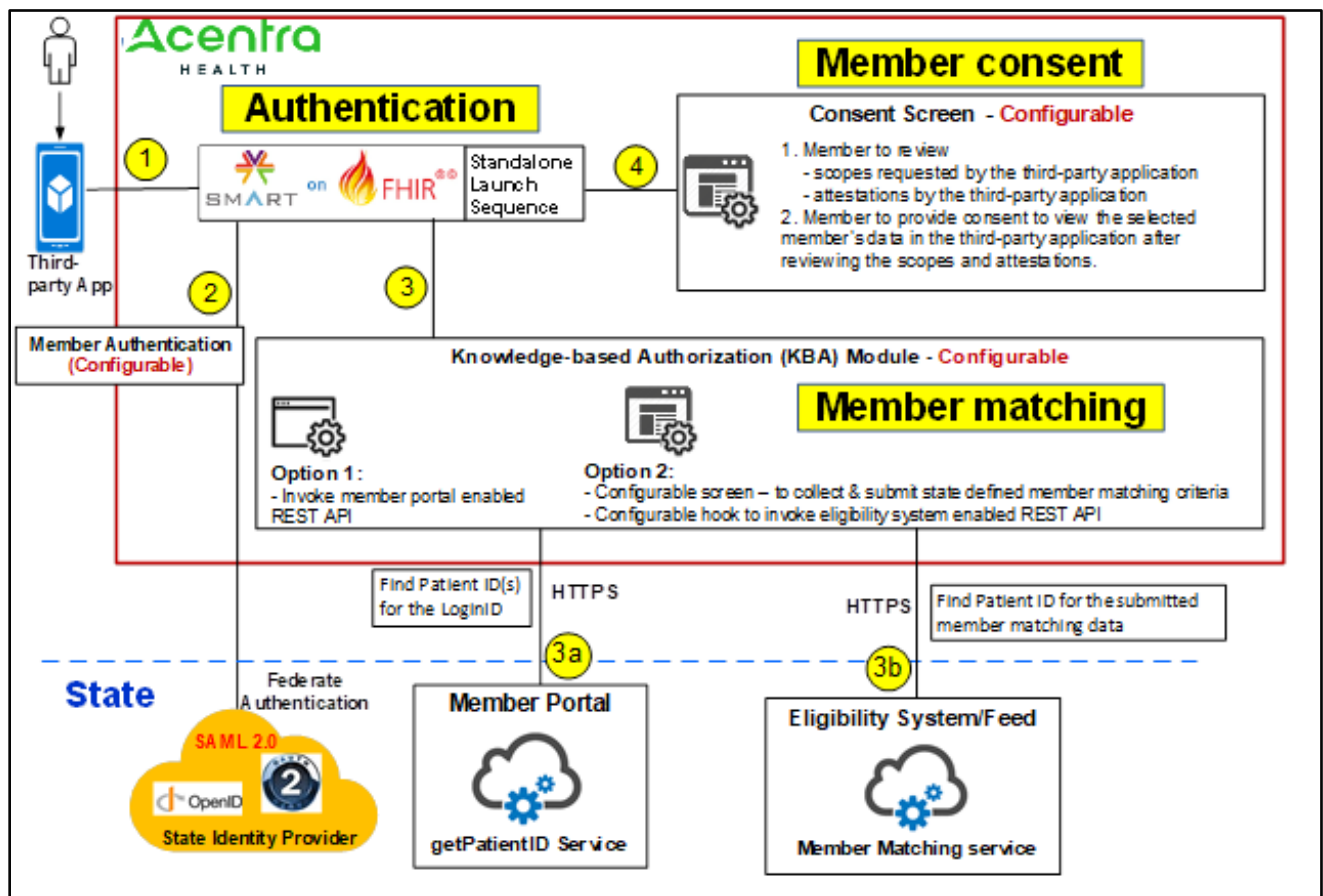


Figure 4. Acentra Sandbox Environment – Member authentication, matching and consent

- Step#3:** The KBA module integrated with the SoF module enables authorization flow to authorize the patient and any authorized caregivers to determine the level of access based on eligibility and state regulations. The KBA module is configurable to support two options:

Option#1 (Step#3a): Invoke the REST APIs enabled by the payer's patient portal to obtain the patient IDs that are accessible for the logged-in patient or the authorized caregivers.

Option#2 (Step#3b): Render a configurable user interface screen within the third-party app, to collect payer defined unique information from the patient and invoke the REST APIs enabled by the payer's eligibility System.

4. **Step#4:** Obtain consent from the patient and any authorized caregivers for what healthcare data can be shared and whom it can be shared with.

Here are a few important user interface (UI) elements that will be rendered inside the third-party app.

3.1 Identity Provider's Login Screen

Acentra's Interoperability Solution enables Identity Federation for Patient Access API. The Acentra solution can integrate with any IdP that supports SAML 2.0 or OIDC (OAuth2) based Identity Federation.

As part of the Identity Federation flow, the Identity Provider's **Login** screen will be rendered to the user inside the third-party app. Figure 4 shows a sample **Login** screen. The Identity Provider may use multi-factor authentication. Due to the Identity Federation, the authentication process between the Identity Provider and the user is transparent to the Acentra Interoperability Solution.

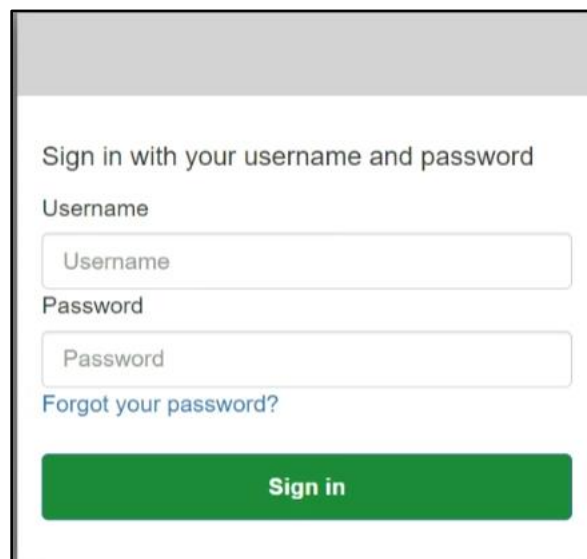
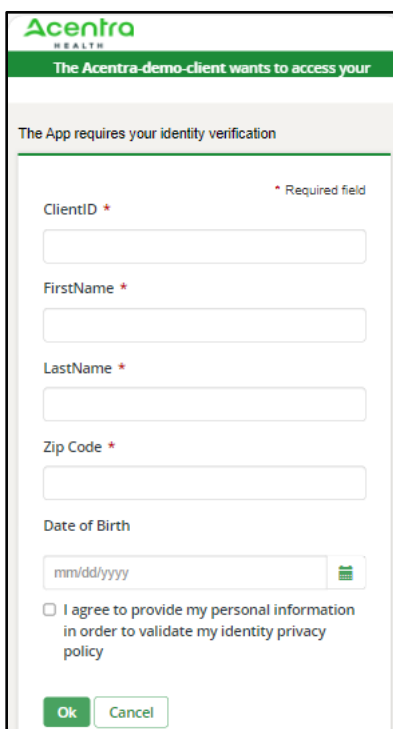


Figure 4. Acentra Interoperability Solution – Login Screen (example)

3.2 Knowledge-Based Authorization (KBA)

Figure 5 shows a sample **KBA** screen (if KBA module is configured to use Option#2) provided by the Acentra Interoperability Solution and will be rendered within the third-party app. This screen is configurable to meet the requirement of patient matching criteria of the payer System.

The image shows a mobile application screen for Acentra Health. At the top, the Acentra Health logo is displayed. Below it, a green banner reads "The Acentra-demo-client wants to access your". Underneath, a grey box states "The App requires your identity verification". The main form area contains several input fields, each with a red asterisk indicating it is a required field. These fields are labeled "ClientID", "FirstName", "LastName", "Zip Code", and "Date of Birth". The "Date of Birth" field has a date picker icon. Below the input fields, there is a checkbox with the text "I agree to provide my personal information in order to validate my identity privacy policy". At the bottom of the form, there are two buttons: "Ok" and "Cancel".

Acentra
HEALTH

The Acentra-demo-client wants to access your

The App requires your identity verification

* Required field

ClientID *

FirstName *

LastName *

Zip Code *

Date of Birth

mm/dd/yyyy

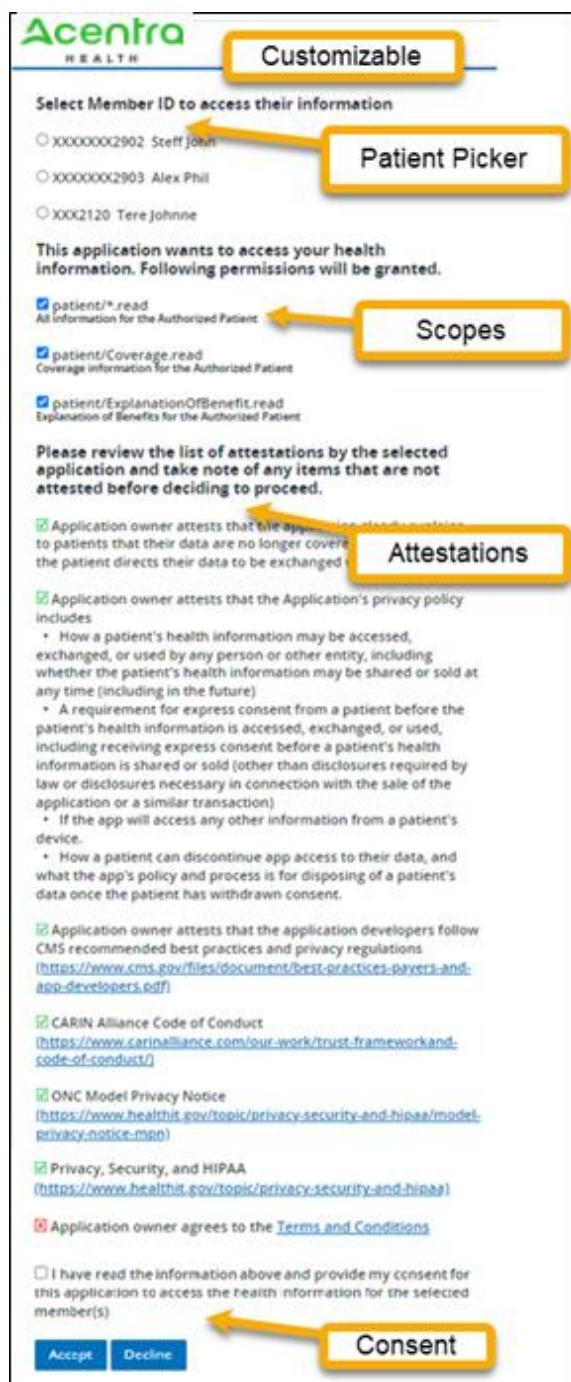
☐ I agree to provide my personal information in order to validate my identity privacy policy

Ok Cancel

Figure 5. KBA Screen (example)

3.3 Consent Screen

Figure 6 shows the **Consent** screen provided by the Acentra Interoperability Solution and will be rendered within the third-party app.



The screenshot shows the Acentra Health Consent screen. It includes a header with the Acentra Health logo and a 'Customizable' label. The main content area is titled 'Select Member ID to access their information' and lists three members: 'XXXXXXX2902 Steff John', 'XXXXXXX2903 Alex Phil', and 'XXX2120 Tere Johnne'. A 'Patient Picker' label points to this list. Below the list, a section titled 'This application wants to access your health information. Following permissions will be granted.' lists three permissions: 'patient/*_read', 'patient/Coverage.read', and 'patient/ExplanationOfBenefit.read'. A 'Scopes' label points to this list. Below the permissions, a section titled 'Please review the list of attestations by the selected application and take note of any items that are not attested before deciding to proceed.' lists several attestations, including 'Application owner attests that the application... to patients that their data are no longer covered... the patient directs their data to be exchanged', 'Application owner attests that the Application's privacy policy includes...', 'Application owner attests that the application developers follow CMS recommended best practices and privacy regulations', 'CARIN Alliance Code of Conduct', 'ONC Model Privacy Notice', 'Privacy, Security, and HIPAA', and 'Application owner agrees to the Terms and Conditions'. An 'Attestations' label points to this list. At the bottom, there is a checkbox for 'I have read the information above and provide my consent for this application to access the health information for the selected member(s)' and two buttons: 'Accept' and 'Decline'. A 'Consent' label points to these buttons.

Figure 6. Consent Screen

The **Consent** screen serves three purposes:

1. Obtain consent from the user to provide the information requested by the third-party app.
2. Provide patient picker functionality, for instance, enable the user to select the patient (self or dependent) associated with the user's login ID.
3. Make the user aware of the CMS-recommended attestations that the third-party application has agreed or denied.

To associate with another dependent, click the **Associate Dependent** link on the **Consent** screen. This will launch the **KBA** screen where the user can go through the KBA process for the dependent to perform the member matching and associate the dependent with the user's login ID.

Note: A dependent's details will only be displayed if their age is less than or equal to 12. If the dependent is 13 years of age or older, their information will not be displayed to the user.

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/secret) 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.

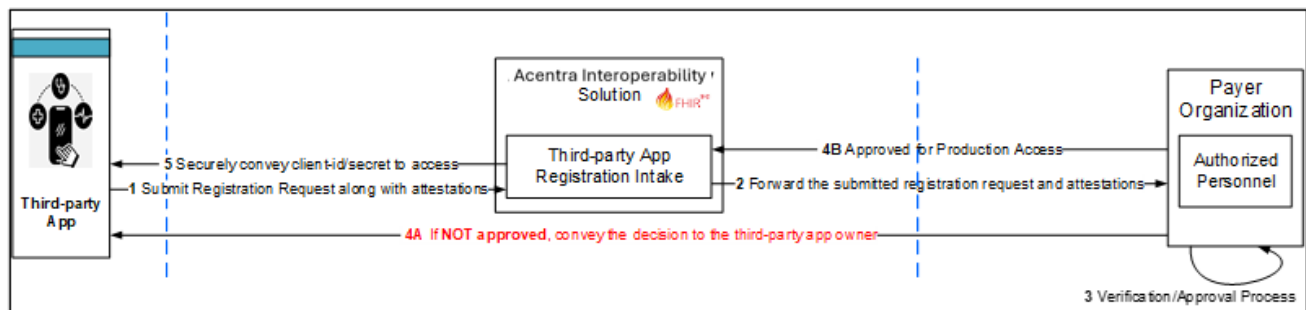


Figure 7. Third-Party App Registration Process

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 9115-F and 0057-F.
Knowledge-Based Authorization	A method of authorizing that seeks to prove that the user is authorized to access the information for self or another individual.
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 (patients).

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
CPCDS	Common Payer Consumer Dataset

Acronym	Definition
CPI	Common Payer Interface
EDI	Electronic Data Interchange
EOB	Explanation of Benefits
FHIR	Fast Healthcare Interoperability Resources
FPDR	FHIR Ready Payer Data Repository
ID	Identification
IG	Implementation Guide
HIPAA	Health Insurance Portability and Accountability Act
KBA	Knowledge-Based Authorization
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
UI	User Interface
URL	Uniform Resource Locator
USCDI	United States Core Data and Interoperability