Acentra HEALTH

Patient Authentication, Matching, and Consent

Unique Challenges for FHIR®

POINT OF VIEW WHITE PAPER

Accelerating Value Through Standards and Re-use of Investments

BACKGROUND

The 21st Century Cures Act, the ONC Cures Act Final Rule, and the CMS Interoperability and Patient Access rule collectively requires CMS covered entities to enable the secure exchange of patient's healthcare information via HL7® FHIR® Application Programming Interfaces (APIs), while ensuring the patient remains in charge of all decisions around their healthcare data.

CMS requires covered entities to authenticate patient identity, grant access authorization, and obtain patient consent to exchange their healthcare information with the application or entity of their choice. This ensures compliance with the Health Insurance Portability and Accountability Act (HIPAA).

FHIR® interoperability ecosystem users connect to the payer's FHIR® server through the 3rd party application of their choice. The 3rd party application only initiates the SMART® on FHIR® compliant 'authorization request' with the FHIR® server. Before any information is released to any 3rd party app, the FHIR® server needs to perform following:

1. Authenticate the patient and any authorized caregivers against an identity verification system that meets federal government's technical and policy controls for privacy and information security.
2. Authorize the patient and any authorized caregivers to determine level of access based on eligibility and state regulations.
3. Obtain consent from the patient and any authorized caregivers for what healthcare data can be shared and whom it can be shared with.

CHALLENGE 1: PATIENT AUTHENTICATION

When it comes to patient authentication, 3rd party apps rely on the FHIR® server to authenticate the patient and any authorized caregivers. Today, the payer's FHIR® servers perform authentication with the payer's identity management system. Maintaining credentials with multiple payers is already challenging for most patients and their authorized caregivers.

The two largest health information exchange networks – The Commonwell® and CareEquality® are moving to identity proofing. The National Institute of Standards and Technology's (NIST) Identity Assurant Level 2 (IAL2) requires any identity verification system (IMS) to identity proof a user using biometric and mobile security requirements of identity proofing is expensive, time consuming, and outside most payers business focus.

THE SOLUTION

Acentra Health's interoperability solution eases these challenges by offering a configurable way to integrate any IMS that uses SAML 2.0 or OAuth 2.0. This flexible solution keeps payers compliant with minimal system impacts by using a single source of authentication.

Figure 1 shows the authentication flow enabled by Acentra Health's interoperability solution that makes this possible. Third-party applications initiate an 'authorization request' with Acentra Health's interoperability solution's SMART® on FHIR® (SoF) module.

As shown in step 2 of Figure 1, the SoF module enables configurable integration with any Identity Management System (IMS) that supports industry standard SAML 2.0 or OAuth 2.0. It also initiates the 'federated authentication flow' with the Identity Provider. The configurable integration identity verification system provides flexibility for the payers to federate authentication. It also allows payers to leverage existing IMS investments IMS, or federate authentication with already established and recognized technology partners, such as ID.me or Login.gov, to meet IAL2 and NIST 800-63-3 standards.

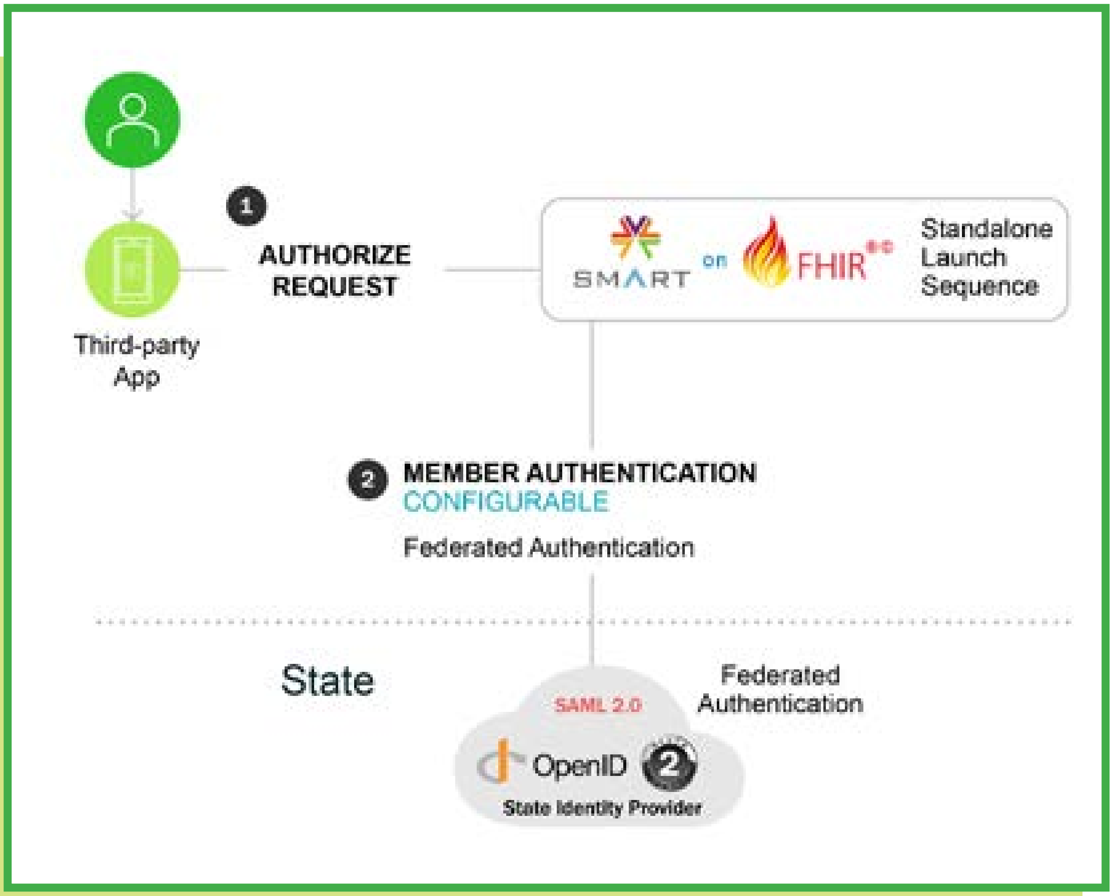


Figure 1. Patient Authentication – Step #1 & 2

CHALLENGE 2: PATIENT MATCHING

The SMART® on FHIR® (SoF) standard requires the return of both an authorized patient ID and an OAuth token-based authorization response. In most cases, the Enterprise Identity Management systems do not maintain payer specific data like the Patient ID (e.g., Medicaid ID) of the patient. This poses a challenge for FHIR implementations and requires "patient matching" to be performed for the logged-in patient and any authorized caregivers to retrieve the unique patient IDs based on the eligibility data.

THE SOLUTION

Acentra Health's interoperability solution includes a Knowledge-Based Authorization (KBA) module that is integrated with the SoF module and authorization flow. The KBA module enables a configurable user interface to collect payer defined unique information from the patient and invoke the REST APIs enabled by the payer's eligibility system or patient portal to validate the patient provided information.

This eliminates the need for multiple sources of authorization from various apps, instead centralizing the process. This is illustrated via step 3 in Figure 3.

In this interface, payers retain the business logic. This setup is preferred by most payers since they own the web service that determines which patient IDs are accessible for the logged-in patient and any authorized caregivers.

Similarly, the KBA module can support consumption of the Da Vinci Health Record Exchange (HRex) implementation guide (IG) defined "member-match" operation that allows one health plan to retrieve a unique identifier for a patient from another health plan using a patient's demographic and coverage information.

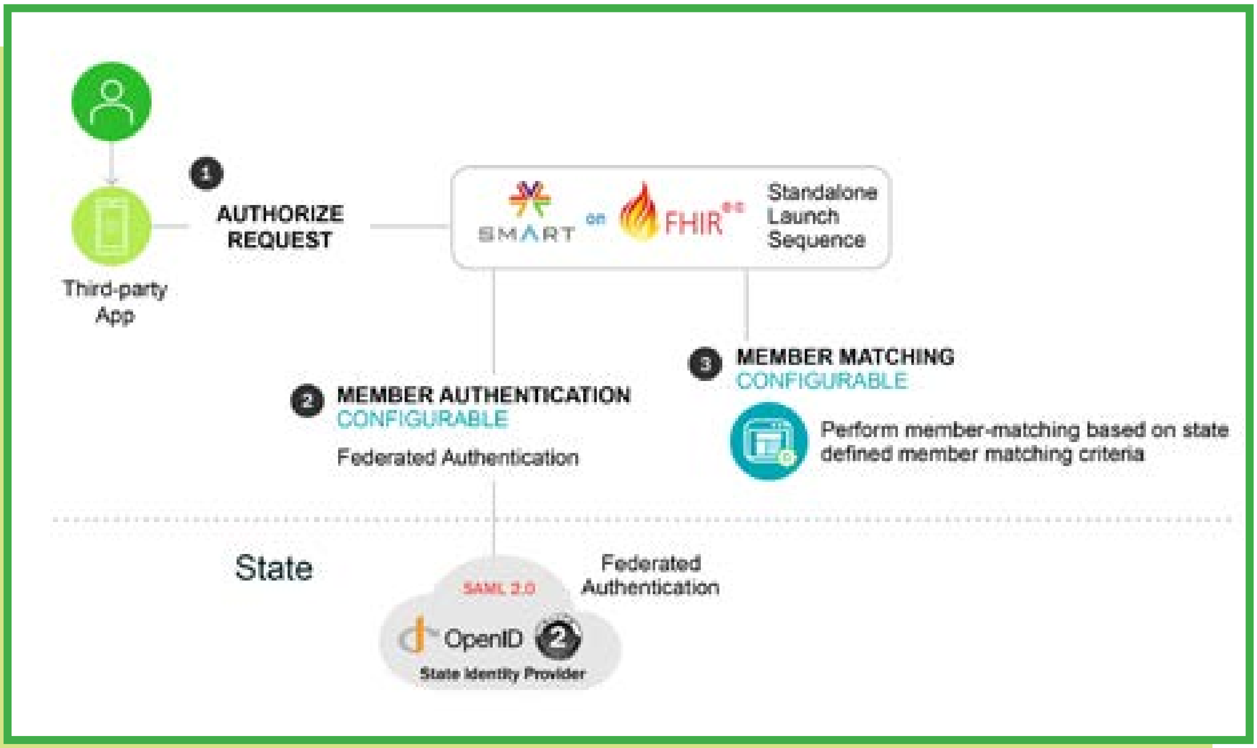


Figure 2. Patient Matching – Step #3

CHALLENGE 3: PATIENT CONSENT

CMS promotes a patient-centric process, where the patient is in-charge of choosing what 3rd party app to use and what data to exchange with the app or other entities. CMS also requires the payers to display the 3rd party application's attestations to the logged-in patient and any authorized caregiver so they can make an informed decision on allowing the 3rd party application to view their healthcare information.

THE SOLUTION

Acentra's Interoperability solution's KBA module enables a fully configurable 'Patient Consent/Patient Picker' module that is also integrated with the SoF module and SAMRT® on FHIR® authorization flow.

Once the patient and any authorized caregivers are authenticated and authorized (steps 1, 2, and 3) the KBA module invokes the 'Patient Consent/Patient Picker' screen in step 4 in the Figure 3.

The 'Patient Consent/Patient Picker' screen illustrated in Figure 4 is customizable and is delivered within the third-party application by the CNSI interoperability solution. It consists of three parts:

- Patient picker
- Scopes
- Application attestations

Part one is the 'patient picker' which lists the Patient IDs retrieved as part of the "Patient Matching" (step 2). The logged-in patient and any authorized caregivers are presented with options of Patient IDs to choose from. They need to select the patient ID whose healthcare data will be shared with the 3rd party app or entity of their choice.

Part two of the screen lists the 'scopes' which is the type of data the 3rd party app is requesting to access. For example, the patient's personal information, Coverage, Explanation of Benefits, and so on. The patient and any authorized caregiver can then select or deselect the boxes in the list to authorize exchanging that information or deauthorize it.

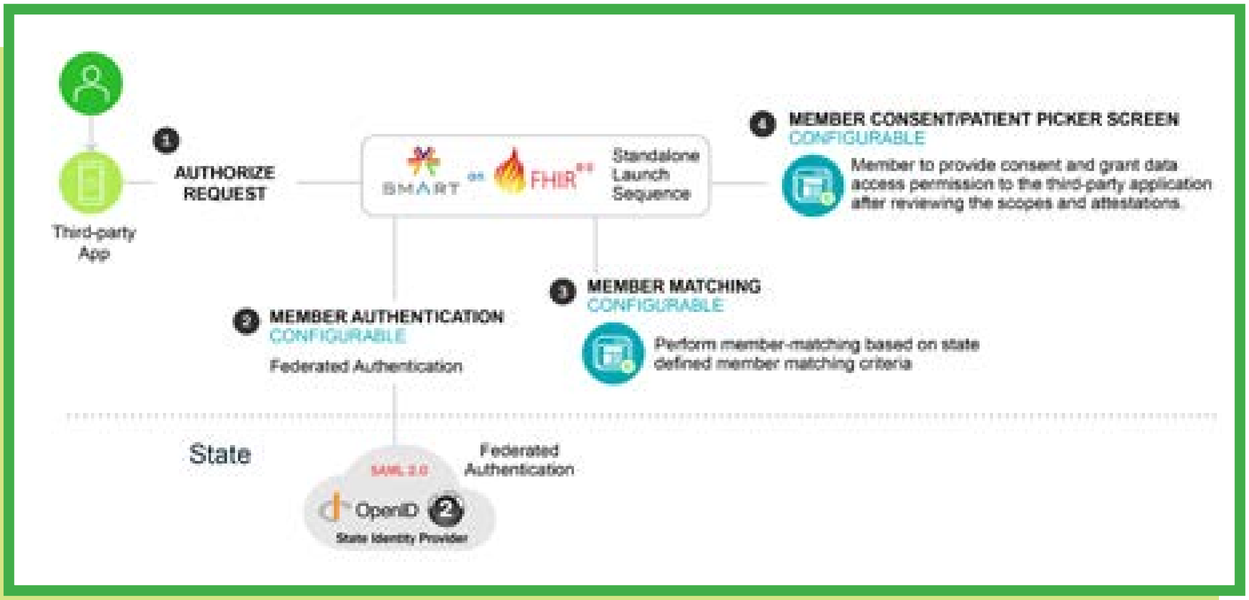
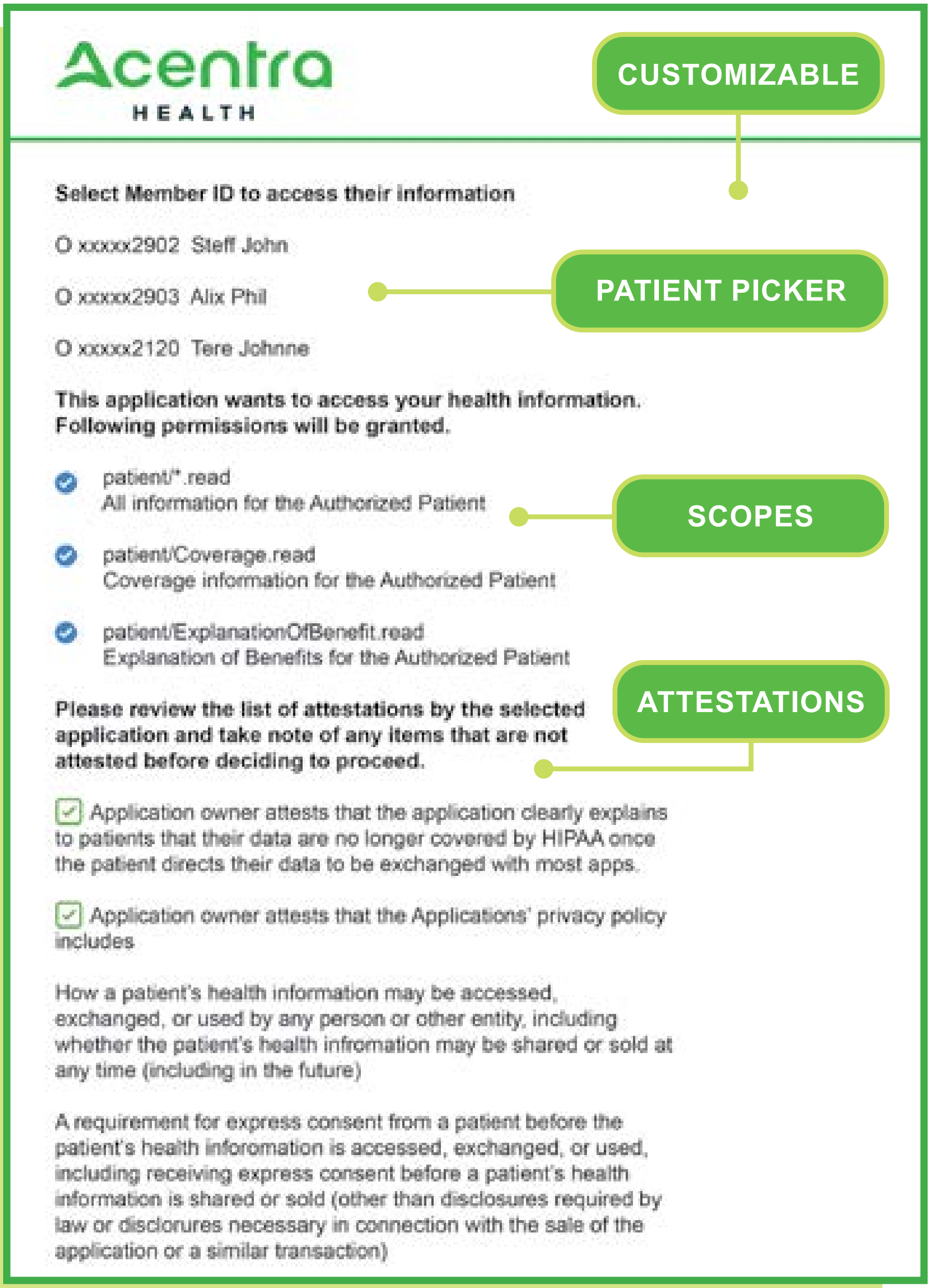

1
AUTHORIZE REQUEST
Third-party App
SMART on FHIR
Standalone Launch Sequence
4 MEMBER CONSENT/PATIENT PICKER SCREEN
CONFIGURABLE
Member to provide consent and grant data access permission to the third-party application after reviewing the scopes and attestations.
3 MEMBER MATCHING
CONFIGURABLE
Perform member-matching based on state defined member matching criteria
2 MEMBER AUTHENTICATION
CONFIGURABLE
Federated Authentication
State
SAML 2.0
OpenID 2
State Identity Provider
Federated Authentication

Figure 3. Patient Consent – Step #4

Part three of the screen lists the application attestations. The logged-in patient and any authorized caregiver can review the attestations and make an informed decision if they still want to proceed with the application of their choice.

The SoF module will create and issue the access token based on the Patient ID, patient (or caregiver) selected scopes, and selected attestations – limiting data access to the selected 3rd party application or entity. The options presented in this clear interface empower patients to make informed decisions about their healthcare information sharing.



Select Member ID to access their information

O xxxxx2902 Steff John

O xxxxx2903 Alix Phil

O xxxxx2120 Tere Johnne

This application wants to access your health information. Following permissions will be granted.

✓ patient/*.read
All information for the Authorized Patient

✓ patient/Coverage.read
Coverage information for the Authorized Patient

✓ patient/ExplanationOfBenefit.read
Explanation of Benefits for the Authorized Patient

Please review the list of attestations by the selected application and take note of any items that are not attested before deciding to proceed.

☑ Application owner attests that the application clearly explains to patients that their data are no longer covered by HIPAA once the patient directs their data to be exchanged with most apps.

☑ Application owner attests that the Applications' privacy policy includes

How a patient's health information may be accessed, exchanged, or used by any person or other entity, including whether the patient's health infromation may be shared or sold at any time (including in the future)

A requirement for express consent from a patient before the patient's health inforomation is accessed, exchanged, or used, including receiving express consent before a patient's health information is shared or sold (other than disclosures required by law or disclorures necessary in connection with the sale of the application or a similar transaction)

Figure 4. Patient Consent/Patient Picker

KEY FEATURES

- Standards-based Federated Authentication
  - Enables FHIR ecosystem to delegate patient authentication to Payer's Identity Provider or External Credentialing Service Provider or trust frameworks
- OAuth2 Token-based Authorization
- SMART® on FHIR® support to extend OAuth2 authorization
- Knowledge-based patient matching: Fully configurable hooks
  - Obtain authorized primary and dependent patient IDs by invoking REST APIs enabled by the eligibility system, Patient Portal, or HREX API.
  - Invoke the configurable KBA screen to collect patient authorization information and invoke REST APIs to obtain authorized primary and dependent patient IDs

CONCLUSION

Acentra Health's Interoperability Solution streamlines the unique challenges around Patient Authentication, Patient Matching, and Patient Consent, while staying compliant with the CMS mandated standards such as HL7® FHIR® and SMART® on FHIR®. The solution also enables the payers to support the upcoming digital federated identity initiatives and standards.

It provides the following business benefits:

Payers

Enables payers to leverage their existing investment in the Enterprise Identity Management Systems, leverage their own Identity Management System, or leverage and integrate with already established and recognized technology partners like ID.me or Login.gov to meet IAL2 and NIST 800-63-3 standards

- Enables payers to adhere to Commonwell Health Alliance's requirement to identity proof the patient at IAL2 level by integrating with external credentialing service providers or trust frameworks
- Delegate the complexity of ever evolving security frameworks and standards to Acentra

Patients

- Makes it easier for the patients to continue using their existing credentials with the payer's Identity Management Systems
- Provides flexibility for patients to use an external IAL2 credentialing service (like id.me) to use 'person-centric' digital identity instead of 'organization-centric' digital identity.

Acentra HEALTH

ABOUT ACENTRA HEALTH

Acentra Health, formed in 2023 by the merger of industry leaders CNSI and Kepro, combines public sector knowledge, clinical expertise, and technological ingenuity to modernize the healthcare experience for state and federal partners and their priority populations. From designing and developing advanced claims, encounter, and provider solutions that drive efficiency and cost savings to delivering clinically focused service models for care management and quality oversight, Acentra Health is accelerating better outcomes. Acentra Health is backed by Carlyle (NASDAQ: CG), a global investment firm.

For information on Acentra Health, visit acentra.com.

ABOUT THE AUTHOR

Ajay Tipnis, Principle Architect, Products

REFERENCES

1. https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet
2. https://www.commonwellalliance.org/connect-to-the-network/#core%20services
3. https://hl7.org/fhir/smart-app-launch/app-launch.html