

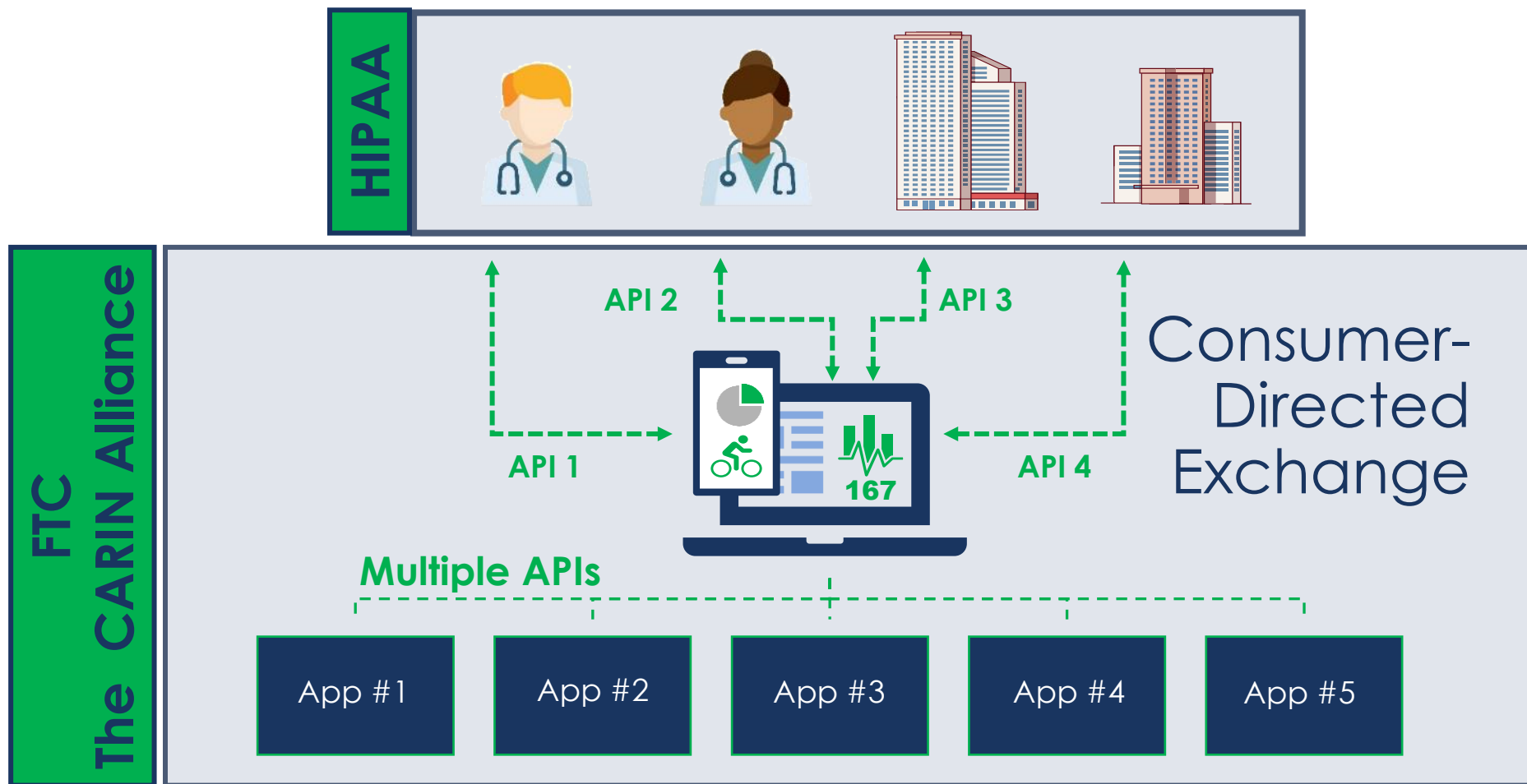
# The CARIN Alliance: Advancing Consumer Directed Health Information Exchange



**LEAVITT**  
PARTNERS



# How will consumers aggregate and share data in the future?





# The CARIN Alliance

## Our Vision

To rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals.



\*Sample list of CARIN members. For a full list of the CARIN board and members go to: <https://www.carinalliance.com/our-membership/carin-board-participants/>



# Consumer's new "digital front door" to health care

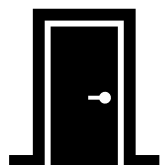


## "The Key"

### Digital Identity and Authentication for the Individual

**What:** Acceptance or creation of an IAL2 identity proofed digital credential

**Solution:** Identity and access management (IAM) solution

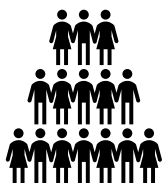


## "The Door"

### Standardized FHIR-based API data exchange

**What:** Standardized clinical, financial, administrative, and SDOH APIs

**Solution:** Development of an API Gateway



## "Community of Problem Solvers"

### B2C health and health care applications

**What:** Innovative applications solving a myriad of health care use cases

**Solution:** A development portal that includes an automated application registration process



## "Your Family"

### Individual consent-based data sharing framework for patients, members, and caregivers

**What:** Consumers consenting to when, where, and how they want to share their data to achieve their goals

**Solution:** An individual proactive, informed, and (ideally) federated consumer-directed, consent-based data sharing framework (As a start: CARIN's Code of Conduct and Trust Framework)



The Key:

**Digital Identity and  
Authentication for  
the Individual**



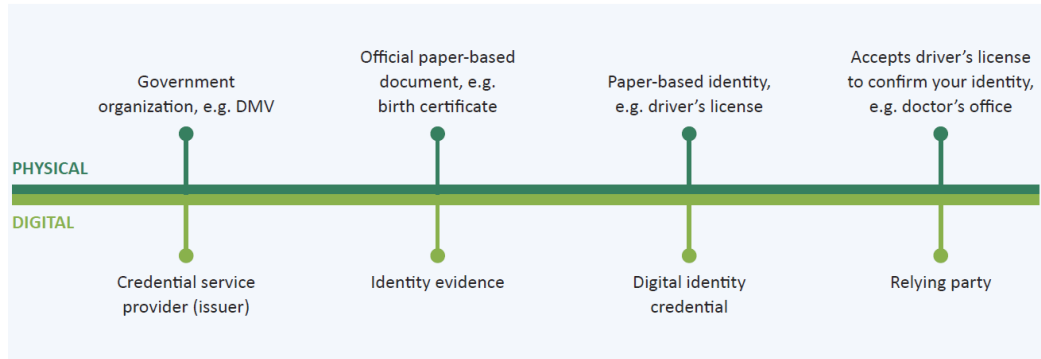
# Federation and Trust

## Digital Identity and Federation in Health Care (Dec 2020)



### IDENTITY CREDENTIALS IN PHYSICAL WORLD VS. DIGITAL WORLD

To illustrate the principle of a “person-centric” identity in the digital world, we can describe it in terms of the process in the physical world now. In today’s physical world, an individual who wants to establish a digital identity credential for a specific authorized purpose will go to a “trusted source” – a credentialing service provider (issuer), which is likely a state or federal government agency – to prove they are who they say they are. In the case of a driver’s license, the individual will go to their state department of motor vehicles who has the authority to issue a driver’s license (paper-based identifier). The state requests that the individual prove they are who they say they are using paper-based document from other third parties who have validated identifying information about the individual; for example, birth certificates, passports, mortgage papers, utility bills, etc. (identity evidence). After those documents have been validated, the individual receives a physical driver’s license (digital identity credential) that can be used as a single, trusted identity credential anywhere in the physical world when someone is required to prove their identity (relying party). The challenge is that sharing everything on your driver’s license for every use case when you are sharing your identity with a relying party often results in oversharing of information. Creating a digital identity credential can help in avoiding oversharing by allowing individuals to only share the specific identity evidence needed to fulfill a specific use case.



It is possible to replicate this process in the digital world to create a digital identity credential, but there are challenges. Digital identity is a relatively new concept, especially in health care. Organizations (relying parties) are hesitant to trust a digital identity credential issued by a credentialing service provider they do not have intimate experience or knowledge of in the same way that they trust a driver’s license issued by a DMV in the physical world.<sup>5</sup> There are trust framework organizations which will certify that the digital identity credential was issued by a credentialing service provider that follows reliable, trusted, and agreed-upon processes; this creates the conditions for digital trust across organizations. In an ideal world, we could use that single digital credential, no matter which trust framework certified the credentialing service provider, to access our health information from different health care organizations, including health plans, providers, and applications. Currently, there are several different trust frameworks that do not have equivalency in the market today, and this restricts the portability of a digital identity credential.



### FEDERATED TRUST AGREEMENT: AN OVERVIEW

#### PURPOSE

Within a trusted federated digital identity ecosystem, there are identity providers or issuers which provide organizational or individual identity products and services. Trust framework organizations are third-party organizations who certify the legal, policy, and technical aspects of the products being provided by the identity providers. A relying party is any stakeholder which needs a trusted identity to exchange data. The CARIN Alliance seeks to develop a digital federated trust agreement which outlines the technical, policy, legal and certification guidelines necessary for equivalency to link each of the trust framework organizations together. The benefit of this approach is that a relying party, which needs a verified identity to authorize access to health data, can trust and rely on an identity credential provided by any identity provider who has been certified by a trust framework organization who participates in the federated trust agreement.

The Federated Trust Agreement will address standardization and best practices related to security, data protection, authentication, identity proofing, privacy, user experience, interoperability and the conformance regime to ensure these specifications and policy obligations are certified and enforced by the trust framework organization. While our paper addresses a specific approach for US health care, there could be multiple schemes and technologies associated with a specific trust framework.

### TRUSTED FEDERATED IDENTITY ECOSYSTEM



<https://www.carinalliance.com/our-work/digitalidentity/>

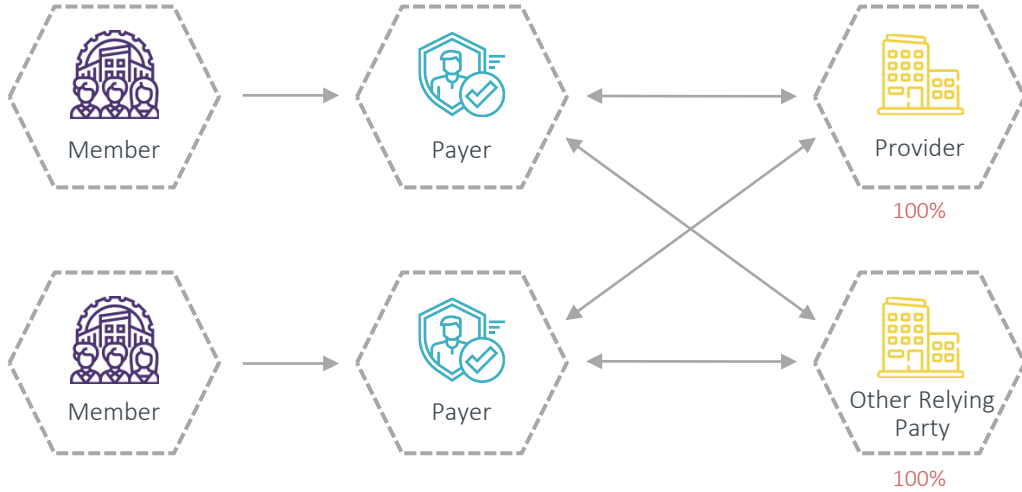


# Federation and Trust

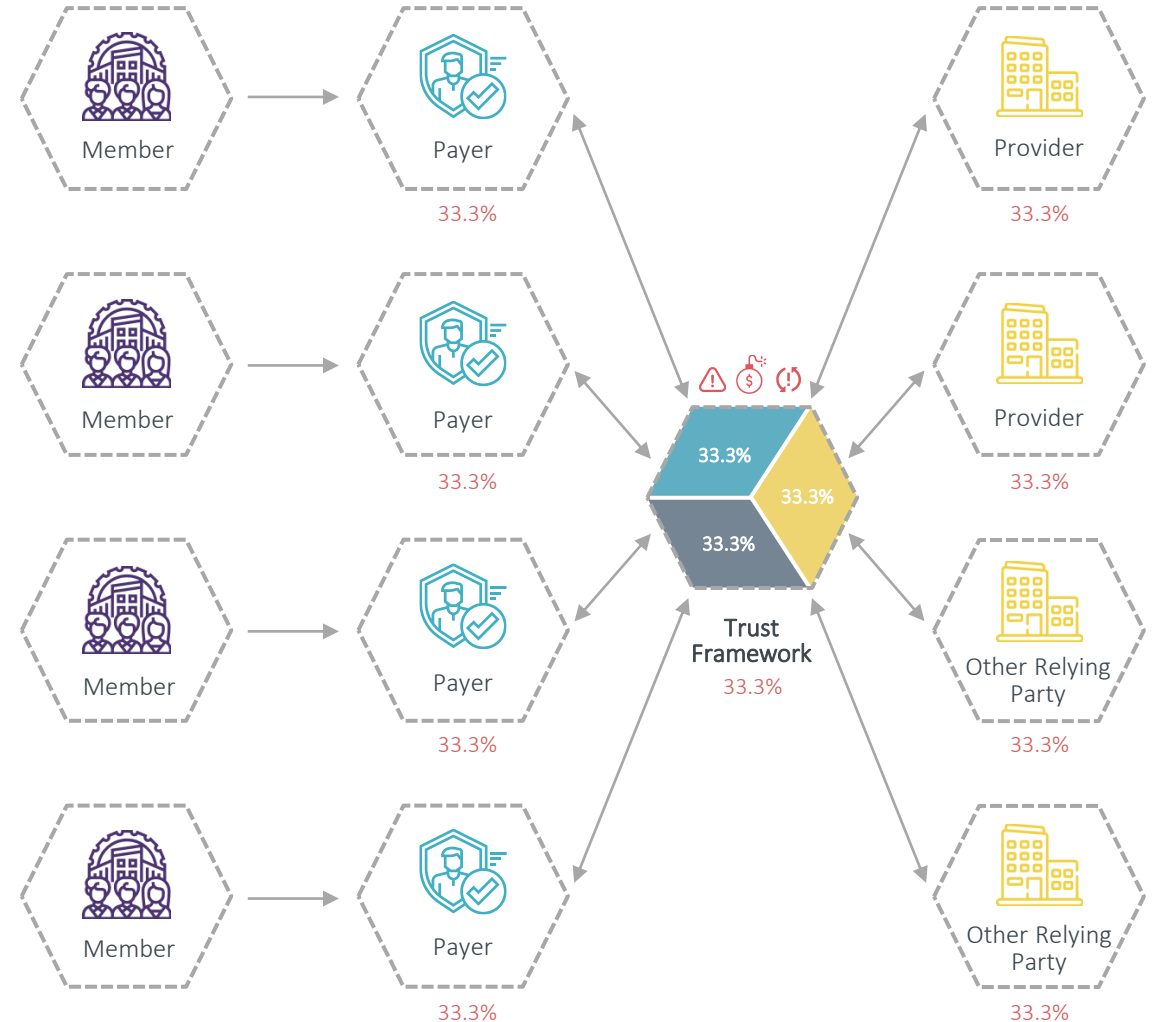
## The Current State of Identity



### Current State



### Future State



#### Risk

Unmanaged or unknown risk that fluctuates between each identity provider



#### Liability

Unmanaged or unknown legal liability unless defined in bi-lateral agreements with each identity provider



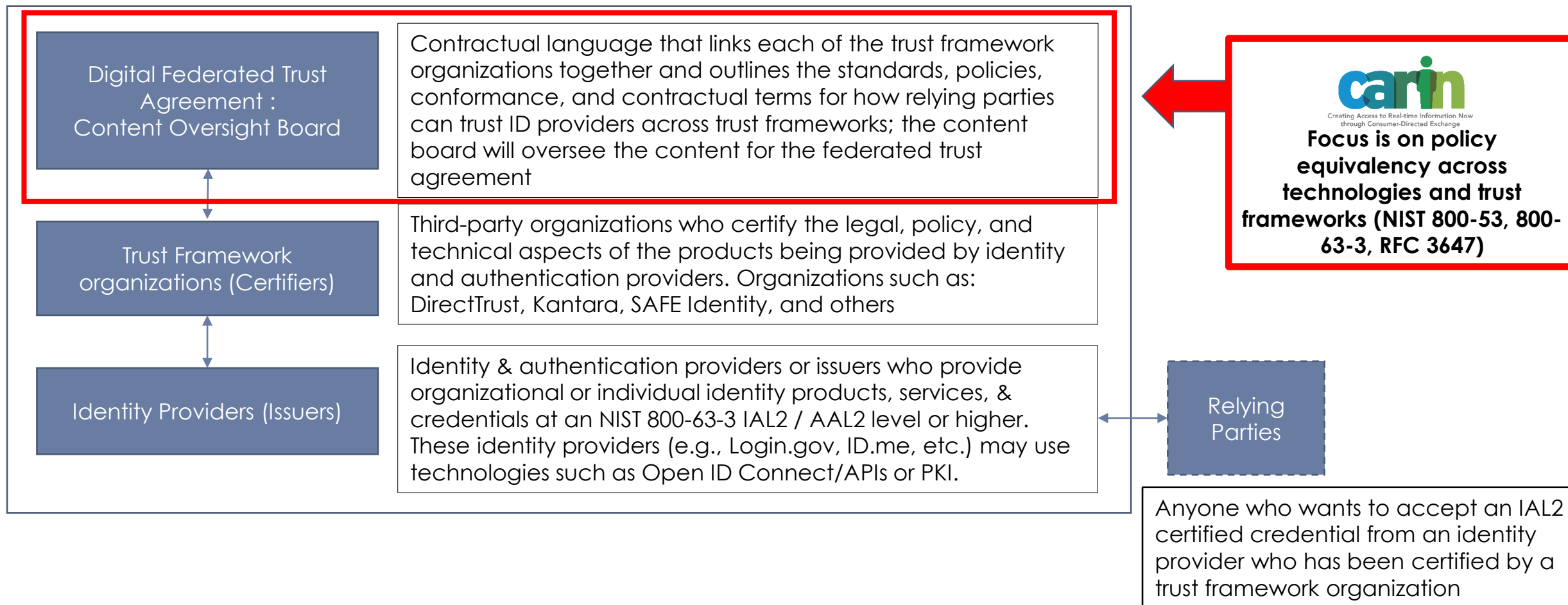
#### Technical Interoperability

Technical interoperability achieved by working with each external entity independently



# Federation and Trust

## Our approach to create a volunteer Trusted Federated Identity Ecosystem



To access the Digital ID and Federation whitepaper, go to:  
[CARINAlliance.com](https://CARINAlliance.com) and select Our Work → Digital Identity → Download our [Digital Identity and Federation White Paper](#)



“The RCE will launch a workgroup of TEFCA stakeholders to develop a model for services that QHINs may offer to support network-facilitated FHIR exchange. The RCE will also coordinate a pilot to test the facilitated FHIR exchange model for Individual Access Services (IAS) and at least one other use case. This pilot is expected to include at least a QHIN, a provider, a payer, and an IAS provider. The results of the pilot will be published by the end of CY 2022 to support publication of the Common Agreement V1.1 and associated Implementation Guides (IGs), as needed, to support full production availability in the first half of CY 2023.”

- “FHIR® Roadmap for TEFCA Exchange, Version 1”, January 2022  
[https://rce.sequoiaproject.org/wp-content/uploads/2022/01/FHIR-Roadmap-v1.0\\_updated.pdf](https://rce.sequoiaproject.org/wp-content/uploads/2022/01/FHIR-Roadmap-v1.0_updated.pdf)



## Objective\*



**Scale an open-source framework for federating trusted Identity Assurance Level 2 (IAL2) certified credentials across health care organizations using a person-centric approach and modern internet technologies.**

\*First announced at our Q4 2021 CARIN Community meeting: <https://www.carinalliance.com/events/carin-community-meetings/>



## HHS XMS

HHS XMS is an identity federation broker tool that enables individuals to choose to log in by selecting from multiple CSPs that have been certified by a trust framework organization.



## Standards

The proof of concept will use NIST-800-63-3, Open ID Connect (OIDC), SMART on FHIR / OAuth 2.0, UDAP, and other open standards.



## Credential Policy

CARIN is drafting a federated credential policy which outlines the technical, policy, legal and certification guidelines necessary to create trust so digital identity credentials can be used and accepted even when they are issued and certified by different credentialing providers and trust framework organizations.



## Participants and Business Operations

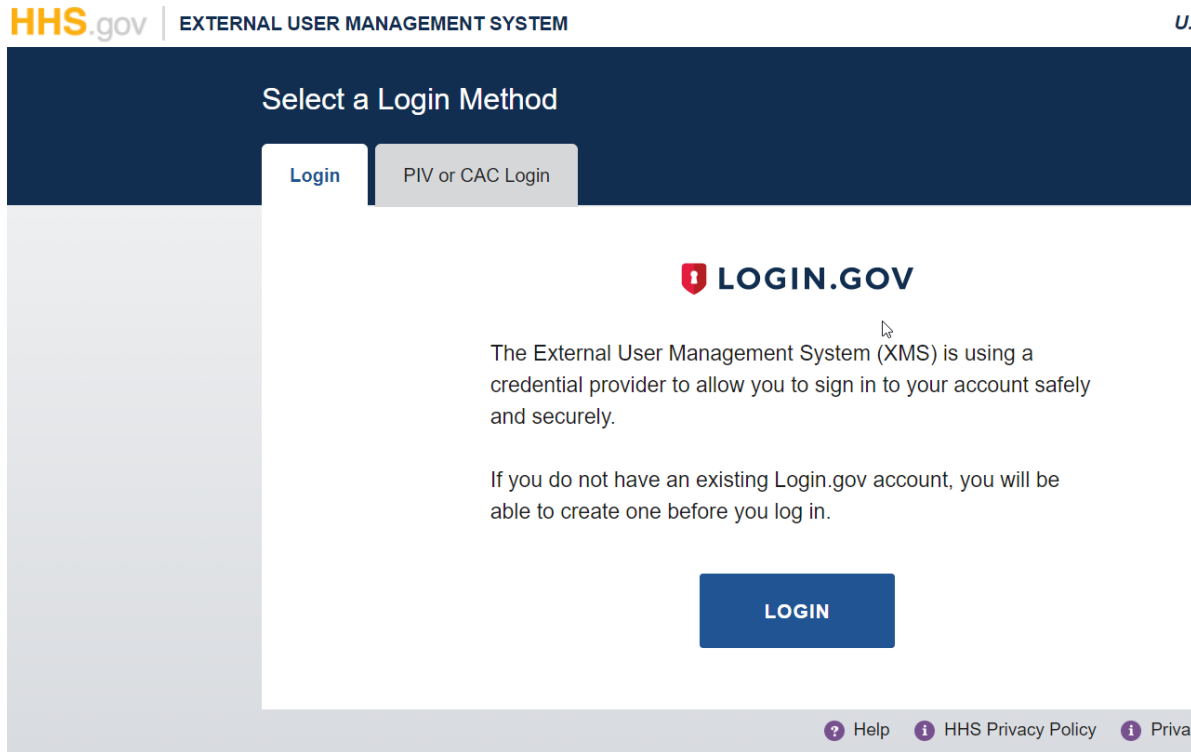
The proof of concept will include applications, health plans, providers, credential service providers, relying parties, and trust frameworks.

# NextGen XMS Walkthrough – Login Page

U.S. Department of Health and Human Services

Users have one of two options for authenticating into XMS (other IdPs who are certified IAL2+ may be added later):

Login.gov credentials:



**HHS.gov** | EXTERNAL USER MANAGEMENT SYSTEM U.S. Department of Health and Human Services

Select a Login Method

**Login** | PIV or CAC Login

**LOGIN.GOV**

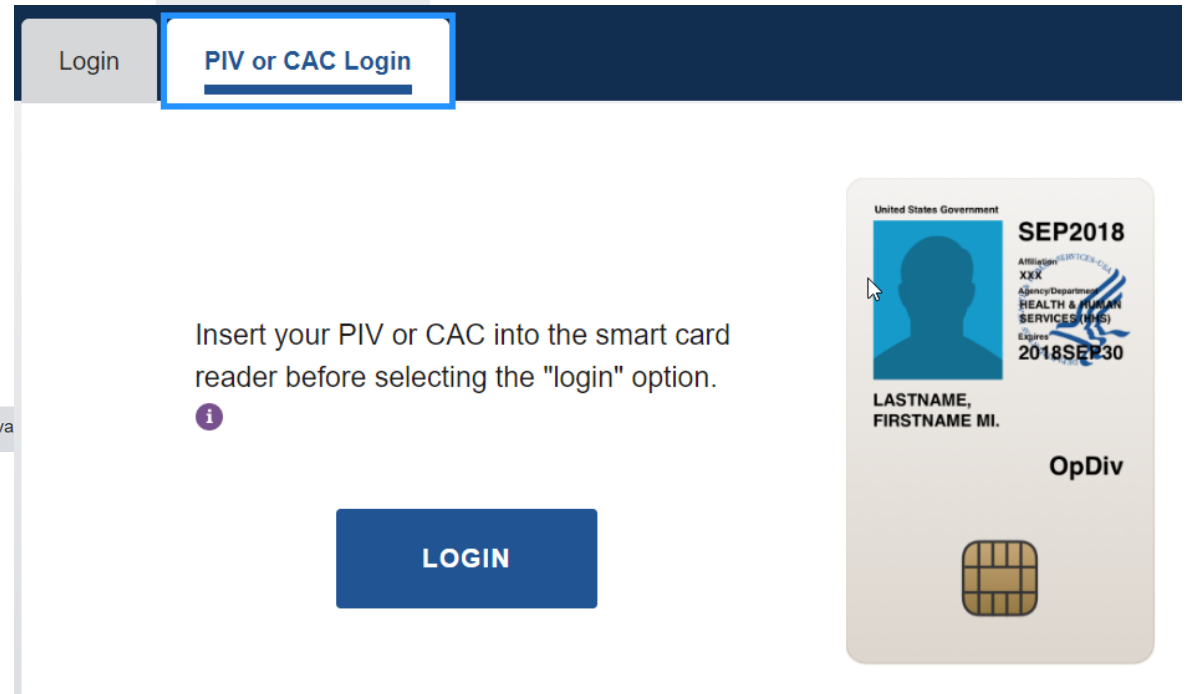
The External User Management System (XMS) is using a credential provider to allow you to sign in to your account safely and securely.

If you do not have an existing Login.gov account, you will be able to create one before you log in.

**LOGIN**

[? Help](#) [i HHS Privacy Policy](#) [i Priva](#)

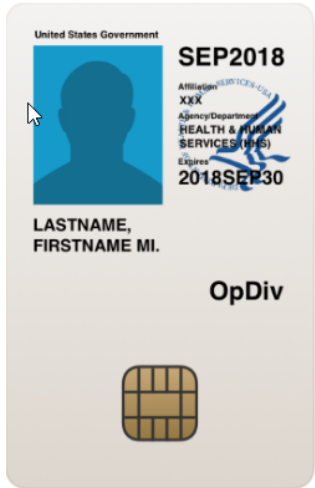
PIV/CAC credentials:



**Login** | **PIV or CAC Login**

Insert your PIV or CAC into the smart card reader before selecting the "login" option.

**LOGIN**



United States Government  
SEP2018  
XXXX  
Agency/Department  
HEALTH & HUMAN  
SERVICES (HHS)  
Expires  
2018SEP30  
LASTNAME,  
FIRSTNAME MI.  
OpDiv



# Cadence and Communication



The bi-weekly meetings will feature technical and policy and governance workstreams.

## TECHNICAL

The technical workstream will address how/whether the proof of concept is working between the relying parties, CSPs, XMS, and Tiered OAuth providers as appropriate.

## POLICY

The policy workstream will ensure the proof of concept is considering the business questions related to what participants need to have in place to go live to trust a digital credential from an organization with whom they may not have a business relationship.

- The proof of concept will also create a private chat through [chat.fhir.org](https://chat.fhir.org) as a primary way of communication.
- The proof of concept leadership team will hold one-on-one meetings with participants as needed.



# Draft Use Cases



## ❖ #1 Consumer-facing Application

- ❖ A consumer uses an application of their choice to identity proof themselves via an IAL2 credentialing service provider and the HHS XMS flow, and then authenticates via XMS to multiple provider and payer FHIR endpoints

## ❖ #2 Health Plan Member

- ❖ A consumer will identity proof themselves via an IAL2 credentialing service provider and the HHS XMS flow, and then authenticates via XMS to multiple applications and providers

## ❖ #3 Health System Patient

- ❖ A patient will identity proof themselves via an IAL2 credentialing service provider and the HHS XMS flow, and then authenticates via XMS to multiple payers and applications

\*\*Similar flows would also occur using UDAP Tiered OAuth but would authenticate using OIDC



# Digital Identity Proof of Concept Participants



ANTICIPATED ROLE	ORGANIZATIONS
Application	b.Well Ciitizen / Invitae OneRecord Otis Health Patient Centric Solutions MaxMD
CSP	AllClear ID – API (Full Service – IAL2/AAL2 in process) ID.me – API (Full Service) LexisNexis – API (Component) MaxMD – PKI Mastercard – API (Component – IAL2) EMR Direct – API
Certificate Issuers	EMR Direct (UDAP Tiered Oauth) MaxMD (UDAP Tiered Oauth)
Identity Broker	Department of HHS XMS team
Relying Party	Cambia Health Solutions (Health Plan) CVS Health (Health Plan) Cedars-Sinai Health System (Provider) Kaiser Permanente (Provider) Marshfield Clinic Health System (Provider and Health Plan) Providence Health System (Provider)
Trust Framework	DirectTrust Kantara Initiative
Government Observer	The Office of National Coordinator (ONC) Centers for Medicare and Medicaid Services (CMS) National Institutes of Health (NIH)



# CARIN Alliance Application Registration Guide

<https://tinyurl.com/24c9rcs9> or the [www.carinalliance.com](http://www.carinalliance.com) home page



Provides a series of best practice recommendation for how applications register with data holders that are centered around 5 specific use cases:

(1) Easily search for and find CMS-regulated payers' respective developer portals, which provide publicly accessible links to all resources needed for them to understand and develop software to interact with the Rule's required API endpoints (Section 5.1).

(2) Testing the required APIs in a sandbox environment (Section 5.2).

(3) Registering with a payer to establish connections with the required APIs in a manner that complies with the Rule (Section 5.3).

(4) Knowing in advance the information a payer will share with members about the developer's application privacy and security practices including template questions related to the CARIN code of conduct (Section 5.4).

(5) Understanding in advance the payers' policies regarding session and refresh tokens, and other service level expectations (Section 5.5).

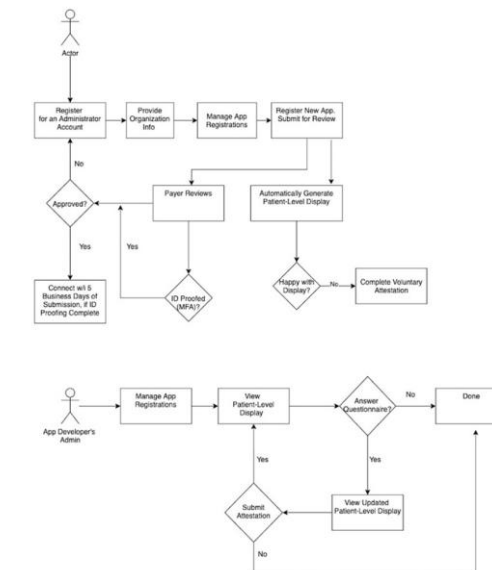
Table 5.3.1 - App Registration Workflow - Information Requested, and Verification Methods

Information Requested	Verification Methods
<b>About the Developer</b>	
What's the legal name for the developer requesting an API connection?	<ol style="list-style-type: none"> <li>1. Check corporate information against public records. <ul style="list-style-type: none"> <li>o Most jurisdictions support business entity search features through their respective corporation departments.</li> </ul> </li> <li>2. Use public or subscription-based business look-up services to validate legal existence.</li> <li>3. Validate the developer's provided email address and phone number.</li> <li>4. Use a recognized third-party legal entity verification service. The CARIN Alliance recommends using the Global Legal Entity Identifier Foundation (GLEIF) which is used and accepted globally across multiple countries, regulators, and industries. (<a href="https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei">https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei</a>).</li> </ol>
What type of legal entity is the requestor (e.g. corporation, partnership, LLC, sole proprietor)?	
Under the laws of what jurisdiction is the entity organized?	
What is the name, job title, phone number and email address for the registrant's primary business point of contact?	
What is the name, job title, phone number and email address for the registrant's primary technical/developer point of contact?	
What is a physical address for the entity (not a P.O. box)? (home address for a sole proprietor)	
What is the URL for the entity's corporate website?	
<b>About the Application</b>	
What is the name of the application?	<ol style="list-style-type: none"> <li>1. Validate information against provid</li> <li>2. Check domains and IP addresses fi URL against blacklists of maliciou: with undesirable and/or illegal acti <ul style="list-style-type: none"> <li>o There are both commercic services available,</li> <li>o An example of one com Anomali, <a href="https://www.anc intelligence-feeds">https://www.anc intelligence-feeds</a>.</li> </ul> </li> </ol>
If different from the developer, what's the legal name for the owner of the application, according to its terms of service and privacy policy?	
Redirect URLs	
As applicable, what is the application's: <ul style="list-style-type: none"> <li>• Homepage URL?</li> <li>• iOS store link?</li> <li>• Android link?</li> <li>• Legal Terms of Service URL?</li> <li>• Privacy Policy URL?</li> </ul>	

4. Transparency –

- a. The Organization includes a publicly accessible link to the Application's Privacy Policy on its website and through the Application.
  - Yes
  - No
- b. The Privacy Policy covers collection, use, and disclosure of [Personal Data](#).
  - Yes
  - No
- c. The Privacy Policy covers collection, use, and disclosure of [De-identified Information](#).
  - Yes
  - No
- d. The Organization provides updates when Privacy Policies have changed, and provides individuals with the option to re-affirm consent or to withdraw consent.
  - Yes

Figure 5.3 - Process Diagram - Registration for Production Environment







# \*New\* CARIN Alliance Code of Conduct UX Guide

<https://carinuxguide.arcwebtech.com>

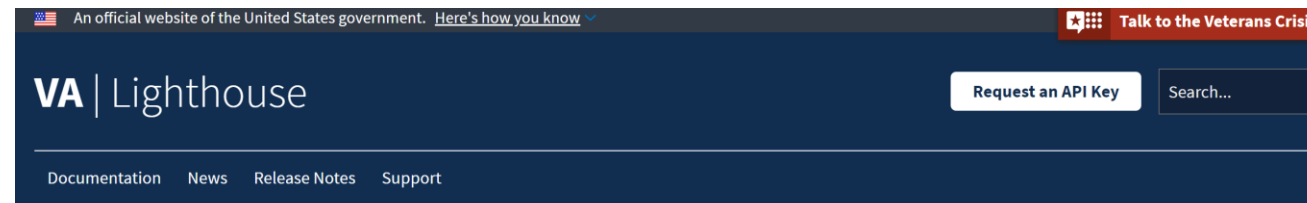


- Multiple consumer-facing applications listed on MyHealthApplication.com are integrating and following the CARIN Code of Conduct
- We need a user-friendly way to display the privacy terms and conditions and application terms of use related to the CARIN Code of Conduct to the consumer.
- Arcweb Technologies, a leader in user experience and design, has co-developed with us the CARIN Alliance Code of Conduct UX guide





# Industry, CMS, & VHA Adoption of the CARIN Code of Conduct



DOCUMENTATION

## Production Access Checklist

A checklist to help your organization prepare to apply for production access to the Blue Button 2.0 API.

### What is this Checklist?

We've created this checklist to help your organization prepare to apply for production access to the Blue Button 2.0 API. We encourage you to consider each of these questions carefully in preparation for your application demonstration for the CMS team and be prepared to discuss your answers. Not all of these questions may apply to your application.

### Basic Information

Over the course of the process, we'll need some basic information about your application:

- What is the name of your organization?
- What is the redirect URI of your application?
- What is the name of the application to which you'd like to connect the BB2.0 API?
- Describe the nature of your application (i.e. how a Medicare beneficiary would use your application)
- When do you hope to release your application for public use?
- How many Medicare users do you anticipate your application will attract?
- Do you have any specific plans to market your application?
- Please list who you'd like the Blue Button 2.0 API team to contact for matters related to your application, such as to set up and attend a demonstration of your application, or answer any follow-up questions we may have about this application?
  - Name(s)
  - Phone(s)
  - Email(s)

### Adherence to the Blue Button 2.0 API Terms of Service & General Privacy Guidelines

The following section is intended to help us understand what your application is doing to protect the sensitive data of Medicare beneficiaries.

#### Ensuring Your Privacy Policy Meets the Basics

- Do you have a privacy policy that is based on industry best practices?
- Is your privacy policy prominent and publicly accessible?
- Please include a link to your publicly available Terms of Service and Privacy Policy.
- Is your privacy policy easy to read, especially from the perspective of a Medicare beneficiary? Or do you explain the privacy policy in another document that is easier to read?
  - If yes, what is the estimated reading level of your Privacy Policy and Terms of Service? How do you know?

#### Ensuring Your Privacy Policy Helps Inform and Protect Medicare Beneficiaries

Does your privacy policy...

- Specify your company's **data collection practice**, including any use and sharing of de-identified, anonymized or pseudonymized data?
- Specify your company's **user consent practice**, including any use and sharing of de-identified, anonymized or pseudonymized data?
  - Note: Some data, even if it has been anonymized, can still be used to identify people with specific medical conditions, etc. Are you doing enough to explain these risks in your privacy policy?
- Specify your company's **data disclosure practice**, including any use and sharing of de-identified, anonymized or pseudonymized data?
- Specify your company's **data access practice**, including any use and sharing of de-identified, anonymized or pseudonymized data?
- Specify your company's **security practice**, including any use and sharing of de-identified, anonymized or pseudonymized data?
- Specify your company's **retention/deletion practice**, including any use and sharing of de-identified, anonymized or pseudonymized data?

## Health API

Use our Health APIs to build tools that help Veterans manage their health, view their VA medical records, and share their information with caregivers and providers. The APIs also provide a Veteran the ability to view their eligibility information that will help them determine if they can receive urgent care and/or community care based on facility proximity and a Veteran's ability to access care.

VA's Veteran Health and Urgent Care Eligibility APIs use HL7's Fast Healthcare Interoperability Resources (FHIR) framework for providing healthcare data in a standardized format. FHIR solutions are built from a set of modular components called "resources." These resources can be easily assembled into working systems that solve real world clinical and administrative problems.

When you register for access to the Health APIs, you will be granted access to a synthetic set of data (provided by the MITRE Corporation) that mimics real Veteran demographics. The associated clinical resources include data generated from disease models covering up to a dozen of the most common Veteran afflictions.

VA is a supporter of the [CARIN Alliance Code of Conduct](#).

Authorization

Community Care

Urgent Care Eligibility



<https://carequality.org/consumer-directed-exchange/>

- MyHealthApplication.com
- Code of Conduct adoption
- Federated Trust Agreement

**CMS 9115-F states**

“Payers can look to industry best practices, including the CARIN Alliance’s Code of Conduct and the ONC Model Privacy Notice for other provisions to include in their attestation request that best meet the needs of their patient population.”



# MyHealthApplication.com and Third-party certification



## Application Gallery

My Health Application

Select an App



Humetrix  
**iBlueButton**

Go to App

DocuSign Envelope ID: 197C38A9-8EA6-4424-9892-14ACC2C28580

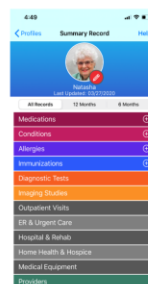
iBlueButton securely aggregates Medicare claim, VA and EHRs with AI powered analytics for individualized care guidelines.

Affiliations  
[CARIN Code of Conduct](#)

Platforms  
[iOS](#)  
[Android](#)

Contact  
[Website](#)  
[Contact Email](#)

Developer Links  
[Privacy Policy](#)  
[Terms of Service](#)  
[Signed Code of Conduct](#)



### We will:

- a) Inform users about their personal data disclosure choices and the consequences of those choices including the risks, benefits, and limitations of data disclosure by providing educational materials ourselves or pointing to appropriate third-party resources.

### ATTESTED BY:

Company	HUMETRIX
Chief Executive Officer (Print)	Bettina Experton
Chief Executive Officer (Signature)	
Date	November 10, 2020



## 1upHealth Patient App

1upHealth

[CARIN Code of Conduct](#)

At 1upHealth, we believe that you should be in control & choose how much data to share and where you want to



## b.well Connected Health

b.well Connected Health

[CARIN Code of Conduct](#)

b.well enables the digital transformation in healthcare. We work with healthcare organizations as the middlewa aggregation, consolidating disparate data and point sol one seamless experience to consumers.



## Buzz Secure Medical Messenger

Skyscape

[CARIN Code of Conduct](#)

Buzz is a HIPAA-secure communications platform for healthcare providers & It Supports live video, texts, calls, audio, images reports.



## Ciitizen

Ciitizen

[CARIN Code of Conduct](#)

Ciitizen is an online platform for patients - beginning with cancer patients - to collect and share their records digitally, free of charge.



## CommonHealth

The Commons Project Foundation

[CARIN Code of Conduct](#)


CommonHealth helps people collect and manage their personal health data and share it with the health services, organizations and apps they trust.

Attestation to the CARIN Code of Conduct now includes **signed versions of the code of conduct** by the application's senior executive

## Certification Progress



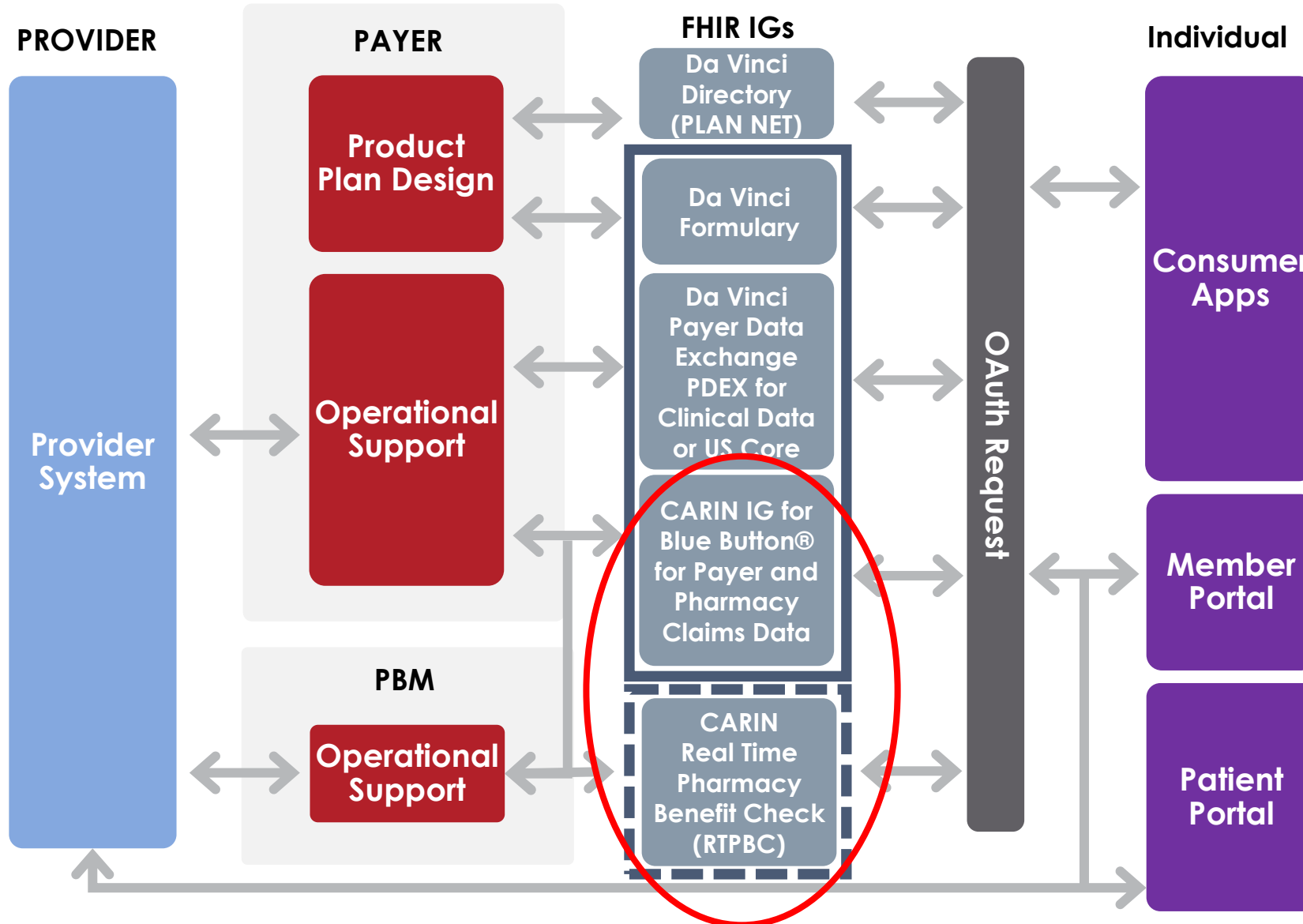
Application **certification programs** have launched which includes attestation and independent certification options



**The Door:**  
**Standardized FHIR-**  
**based API data**  
**exchange**





# CMS final rule: FHIR Implementation Guide (IG) Options



### FHIR Accelerator Commentary

1. Goal is to reduce burden on payers, providers, vendors and patients to meet 6/1/21 req, excludes 1/1/22 requirements
2. There is no specific CMS requirement to use any HL7 Implementation Guide
3. FHIR Community is working collaboratively to ensure the specific guide meets CMS final rule
4. All guides are Draft Standards for Trial Use (DSTU) or moving towards a published version of STU1 or STU2

### Legend

-  CMS Patient Access API for 2021
-  Opportunity to expand CMS Patient Access API for 2022

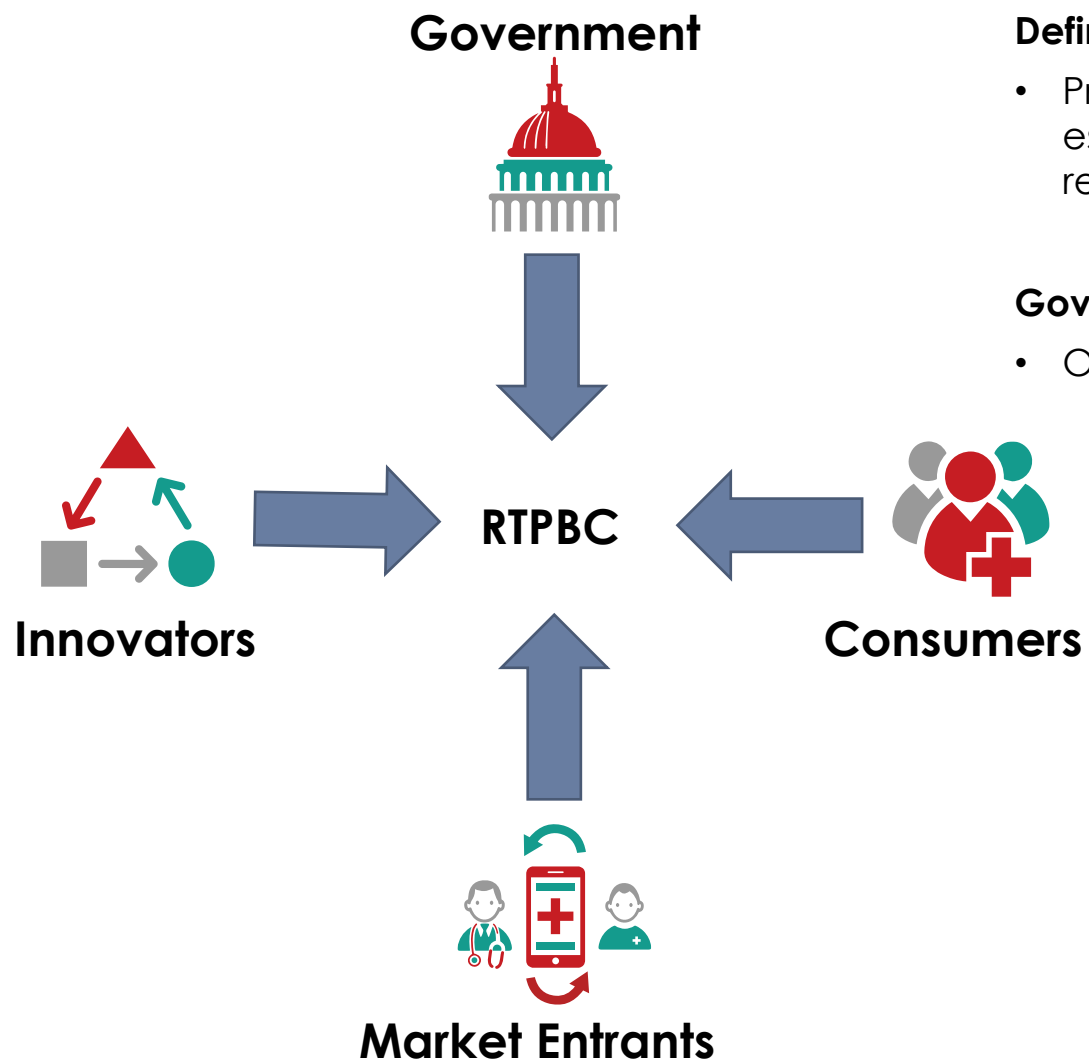


# CARIN HL7® FHIR® Implementation Guides



Implementation Guide	Purpose	Latest Updates	IG Page
<b>CARIN IG for Blue Button® STU1 and STU2 (Health Plan WG)</b>	This implementation guide describes the CARIN for Blue Button® Framework and Common Payer Consumer Data Set (CPCDS), providing a set of resources that payers can display to consumers via a FHIR API to meet part of the CMS requirements related to the Patient Access API.	STU1 published in November 2020. Minor technical corrections were published in early July 2021 as STU1.1.0. We will ballot STU2 in January 2022. Publication in Q1/Q2 2022. At the September HL7 Connectathon and November CARIN testing event a number of clients and servers successfully connected and exchanged the oral and vision types for the first time. We will also test at the January HL7 Connectathon.	<a href="https://build.fhir.org/ig/HL7/carin-bb">https://build.fhir.org/ig/HL7/carin-bb</a>
<b>CARIN IG for Digital Insurance Card STU1 (Health Plan WG)</b>	This guide will develop artifacts (FHIR implementation guides, code mappings, reference implementations, etc) to enable the digital exchange and digital rendering of the elements found on a person's physical insurance card. The primary use case is to support insurance members who wish to retrieve their proof of insurance coverage digitally via a consumer-facing application. Images, barcodes, and QR codes from the physical card will be considered as optional fields for representation within FHIR, but these elements will be optional and up to the implementer to decide whether they want to provide them. The scope of this IG does NOT address eligibility checks between health providers and the insurance company.	The draft IG is now live. Ballot scheduled for January 2022. Publication in Q1/Q2 2022. Implementers also successfully tested at the November CARIN testing event. We will also test at the January HL7 Connectathon.	<a href="https://build.fhir.org/ig/HL7/carin-digital-insurance-card/">https://build.fhir.org/ig/HL7/carin-digital-insurance-card/</a>
<b>CARIN IG for Consumer-facing Real-time Pharmacy Benefit Check STU1 (RTPBC WG)</b>	Provide a patient with real-time pharmacy information associated with their benefit and formulary information, out of pocket costs, therapeutic alternatives, and cash price options.	Published the IG in August 2020. Will be testing with the 5 major PBMs in Q1 2022 after they've built out their support for FHIR by 7/1.	<a href="https://build.fhir.org/ig/HL7/carin-rtpbc">https://build.fhir.org/ig/HL7/carin-rtpbc</a>

# Consumer-facing Real-time Pharmacy Benefit Check



## Definition

- Provide consumers with access to their formulary and benefit information, estimated out of pocket costs, therapeutic alternatives, and cash price in real-time after a provider has prescribed a medication

## Government

- One of few policy agenda items with bipartisan support.
  - Presidential Executive Orders and Drug Pricing Blueprint
  - **Electronic B2B Real-time Benefit Tool or “RTBT”**
    - Addressed in CMS Part D Drug Pricing Final Rule in May 2019 (CMS-4180-F)
    - Required for Part D plans by January 2023
  - **Transparency in Coverage Final Rule (CMS-9915-F) October 29, 2020**
    - “To that end, the final rules require plans and issuers to disclose in element (i), an individual’s out-of-pocket cost liability for prescription drugs, and in element (iii), the negotiated rate of the drug.”
    - Effective January 1, 2022
    - You can use the Consumer-facing real-time pharmacy benefit check API to be in compliance with this rule

Published HL7® FHIR® STU1 version: <https://build.fhir.org/ig/HL7/carin-rtpbc/index.html>



# Questions



## Presenter and Contact Information



Ryan Howells  
Program Manager, CARIN Alliance  
[Ryan.Howells@leavittpartners.com](mailto:Ryan.Howells@leavittpartners.com)

**Request:** We need your developer portal information!! 😊

@carinalliance | [www.carinalliance.com](http://www.carinalliance.com) | [HL7.org/CARIN](http://HL7.org/CARIN)