Q4 2021 CARIN Community Meeting

NOVEMBER 12, 2021

LEAVITT
PARTNERS

Q4 CARIN Community Meeting

Topic	Presenter(s)	Time (ET)
Welcome, Anti-trust reminder, New Members Admitted	Dave Lee, LP	1:00pm – 1:05pm
Leadership Perspective	Aneesh Chopra, CareJourney	1:05pm – 1:15pm
Update: Federal Trade Commission (FTC)	Off the Record	1:15pm – 1:45pm
Patient and Caregiver Perspectives	Anil Sethi, Ciitizen	1:45pm – 2:00pm
HHS / CARIN Digital Identity Proof of Concept	Ryan Howells, LP Adam McBride, HHS Badri Nemani, Deloitte Kyle Neuman, DirectTrust	2:00pm – 2:30pm
Workgroup Update	Leavitt Partners Team	2:30pm – 2:45pm
BREAK		2:45pm – 3:00pm
SMART Health Cards and the Common Trust Network	JP Pollack, The Commons Project Josh Mandel, Microsoft	3:00pm – 3:15pm
Opportunities to Collaborate	Aneesh Chopra, CareJourney	3:15pm – 3:55pm
Next Steps and Adjourn	Ryan Howells, LP	3:55pm – 4:00pm

ANTI-TRUST REMINDER

Please remember that this meeting may include representatives of companies that compete with one another in the marketplace. Discussions, plans, consensus arrangement, agreements, strategies, etc., may be unlawful if they relate to, and should not include, any of the following topics: current or future prices or bidding information; limits on production or product lines; allocating customers or territories; individual company marketing strategies, projections, or assessments; and establishing a practice of dealing with customers or suppliers.

New Members: Welcome!

- Innovaccer (Enabler; www.innovaccer.com)
  - *The Innovaccer Health Cloud unifies patient data across systems and settings, and empowers healthcare organizations to rapidly develop scalable, modern applications that improve clinical, operational, and financial outcomes. Innovaccer's solutions have been deployed across more than 1,000 care settings in the U.S., enabling more than 67,000 providers to transform care delivery and work collaboratively with payers and life sciences companies.*
- Commure (Enabler; www.commure.com)
  - *Building a common architecture for tomorrow's health ecosystem. Our mission is to unite health innovators around open collaboration for scalable care that puts people first.*
- RxRevu (Application; www.rxrevu.com)
  - *Our mantra is inspired by RxRevu's Co-Founder, Dr. Kevin O'Brien, and the story about his mother Lucy and her rising prescription costs. Kevin, a practicing physician, noticed his mother's increasing medication costs and knew he could help. He was able to provide her with medication alternatives to take to her physician and, in doing so, cut Lucy's monthly drug spend in half. This personal story is the foundation upon which RxRevu was built. Everyone here has their "Lucy", and they are the reasons why we work here.*

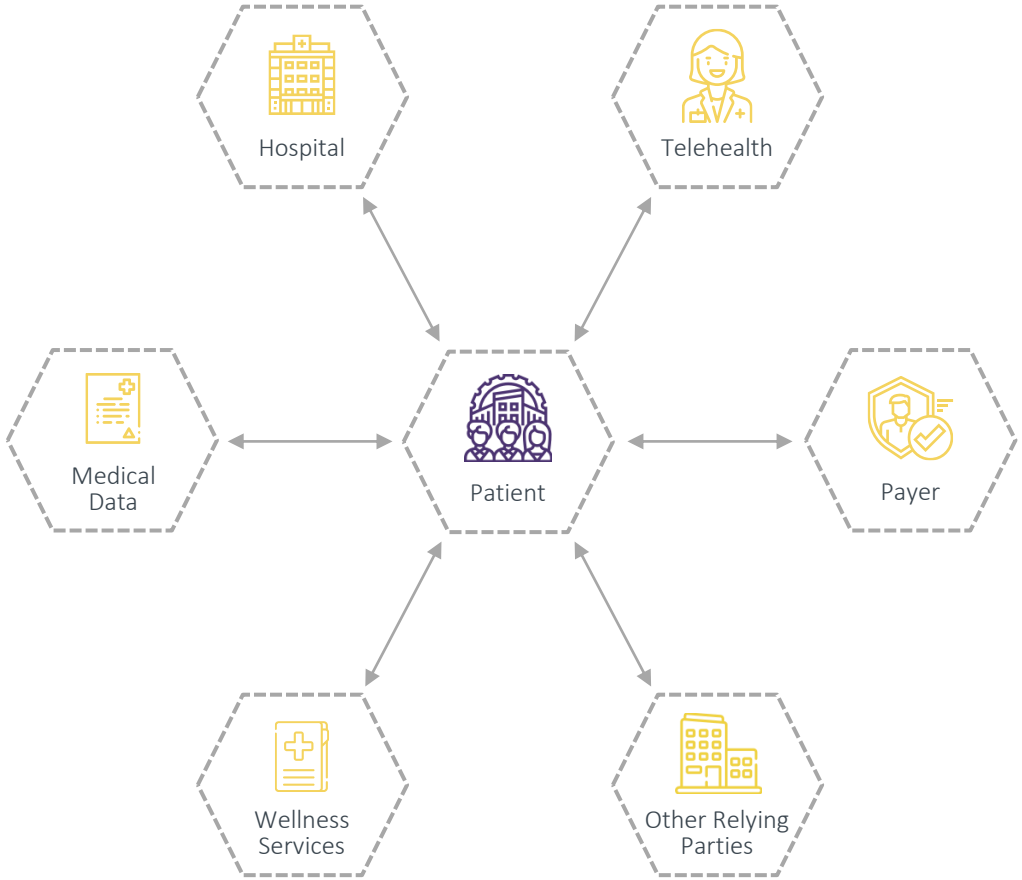
Update: Federal Trade Commission

Patient and Caregiver Perspective

Anil Sethi

HHS / CARIN Digital Identity Proof of Concept

A Person-Centric Approach to Health Data



Give prior authorizations, sign HIPPA disclosures and communicate other information with healthcare providers

Engage in telehealth or renew prescriptions with a physician

Obtain and exchange health information with HDOs, payers, health management apps and other businesses a patient chooses to engage with

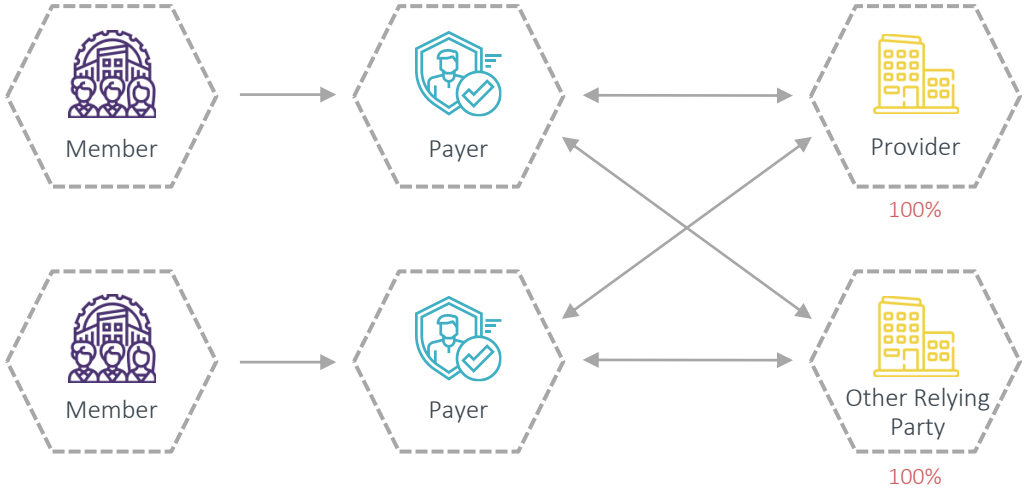
Interact with payers or change payers as patients move between employers, get married or undergo other life changes

Engage with online wellness services, mental health, and other health and healthcare related software systems

Interact with other relying parties that may not be involved in healthcare (e.g., community-based organizations) but are willing to consume identity assertions from health or healthcare-oriented identity providers

The Current State of Identity

Current State

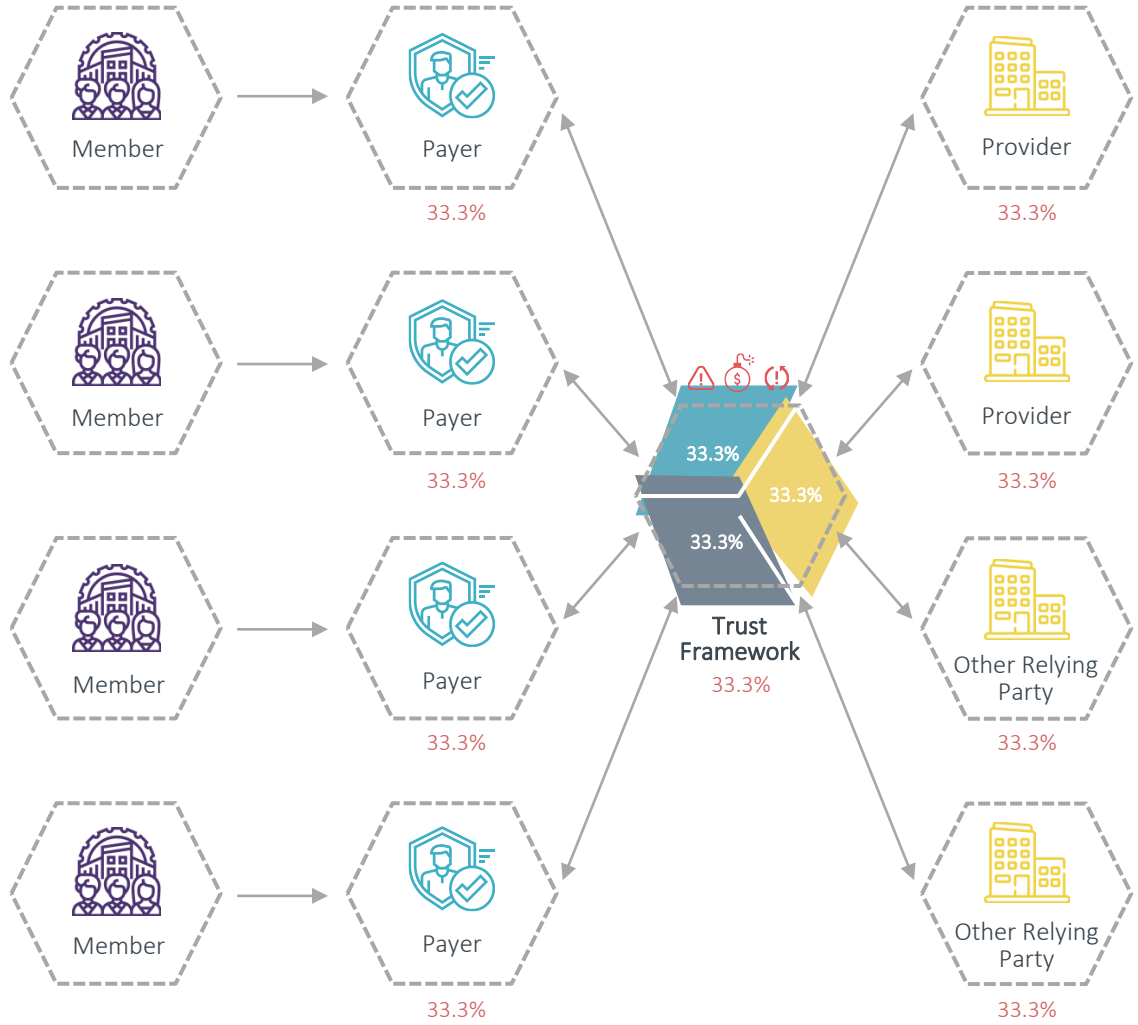


Risk
Unmanaged or unknown risk that fluctuates between each identity provider

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

Future State



Federating Trust is What a Trust Framework Does

Current Approach

- Number of federations increases quadratically for vendors and buyers
- Most security auditors don't know how to audit identity systems
- Establishing legal and liability agreements with all entities is very expensive for both parties
- Lack of global governance leads to inconsistent identity assurance between companies
- Evaluating annual audits of 10s or 100s of identity providers is not viable with limited resources

Trust Framework Approach

- Federate Trust rather than identities
- Enables participants to buy products that support standards in identity and cryptography
- One industry-led governance body to aggregate and manage federations between organizations
- Require vendors to procure or issue their own credentials when engaging in business with you that you can rely on
- Support all identity use cases to include authentication, digital signatures, encryption and IoT for your entire supply chain
- Consolidate liability, warranties indemnification and other legal matters across all vendor identity credentials

Proof of Concept : Vision

Objective: Implement and scale a voluntary, open framework for federating digital identities across relying health care stakeholders using Identity Assurance Level 2 (IAL2) certified credentials, a person-centric approach, biometrics, and modern internet technologies.

Proof of Concept : Foundational Elements

HHS XMS

HHS XMS is an identity federation broker tool that enables individuals to voluntarily 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.

Common 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.

How do we determine trust across credential service providers (CSPs)?

- How well does the CSP know the person they are about to credential?

- What is the availability requirements of the CSP?
- What are the requirements for DR?

- Is the CSP willing to vouch for the integrity of their credentials legally?
- If a credential is mis-issued, and a healthcare organization receives damage, how do they recover?

- How sure is the CSP that they've bound the authenticator to the same person they ID proofed?
- How often is the credential cycled?
- How is the credential revoked?

- What security controls are the CSP audited against to ensure they don't get hacked and issue malicious credentials?
- What kind of auditing data is logged by the CSP?
- How is separation of duties handled?

- How are CSPs evaluated against all of this criteria?
- Who is allowed to do the audits?
- How often are they reviewed for continued adherence to the criteria above?

HHS NextGen External User Management System (XMS)

NextGen XMS is a scalable, cloud-based solution that allows HHS Operational Divisions to focus on their mission and takes into consideration:

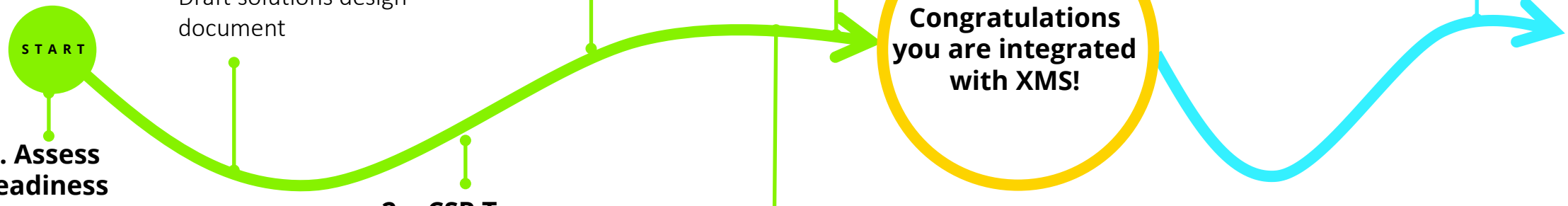
- Alignment with Digital Identity guidelines, ICAM and Cloud modernization efforts
- Security and compliance with federal standards (NIST, OMB, HHS EPLC requirements, etc.)
- Identity and Access Governance and delegated administration model
- Enterprise service that can secure access to external HHS applications
- Centralized platform that is flexible to integrate with third-party providers and services

Capabilities & Benefits

Secure Access:	***Enables external users to access protected applications using credentials issued by the General Services Administration's (GSA's) Login.gov or other agency's PIV/CAC***
NIST 800-63-3 Compliance:	***IAL1, IAL2, and IAL3, and AAL2 and AAL3***
Identity Proofing/Delegated Proofing:	***Remote ID proofing using Login.gov; and delegated proofing for users that affiliate with an organization that's managed within NextGen XMS.***
Organization Affiliation:	***Ability to create and manage organization affiliations within NextGen XMS***
Access Requests/Approvals:	***Configurable access request framework for an application***
Organization Relationship Management:	***Ability to create organizations and manage affiliations to those organizations***
Accredited Platform and Helpdesk:	***NextGen ATO in place which includes Login.gov; no impact to integrated application's ATO, only ISA/MOU required***

XMS Technical Process – Credential Service Provider

As XMS team identifies qualified CSPs, a proof of concept is conducted in the lower environment, followed by the production integration.



0. Assess Readiness

- Protocol support - Support SAML or OIDC protocols for authentication
- Environment support - A non-production environment for integration testing
- Kantara certification for NIST IAL/AAL alignment

1. Initiation/ Planning

- CSP and XMS team aligns on prerequisites, timelines and resources, including UAT testers
- Gather requirements and design from XMS Team
- Draft solutions design document

2a. CSP Team Development

- CSP team reviews solution design document and provides feedback

2b. XMS Team Development

- XMS team begins development for proof-of-concept
- XMS team verifies baseline requirements

3. Testing

- XMS team and CSP conduct integration testing
- Conduct UAT testing

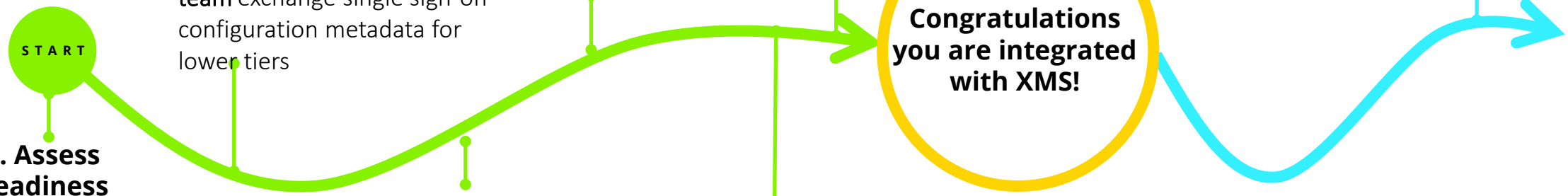
4. Implementation

- CSP and XMS team complete production configuration and coordinate a go-live

5. Ongoing Change Management (ongoing)

XMS Technical Process – Relying Party Application

Application team and XMS team work collaboratively to complete application integration with XMS.



0. Assess Readiness

- Protocol support - Support SAML or OIDC protocols
- Environment support - A non-production environment for integration testing

1. Initiation/ Planning

- **Relying party application team** and **XMS team** aligns on prerequisites, timelines and resources, including UAT testers
- **Application team** and **XMS team** exchange single sign-on configuration metadata for lower tiers

2a. Application Team Development

- **Relying party application team** complete configuration updates and development (if applicable)

2b. XMS Team Development

XMS team complete configuration of relying party in the Integration tier

3. Testing

- **XMS team** and **relying party application team** conduct integration testing for integrated lower tiers
- Conduct UAT testing in the production equivalent tier, specified by the relying party application team

4. Implementation

- **Relying party application team** and **XMS team** complete Operation Readiness Review, production configuration and coordinate a go-live window

5. Ongoing Change Management (ongoing)

Proof of Concept : Interested Participants

ACTIVELY INTERESTED	POTENTIAL PARTICIPANTS
AllClearID	AstraZeneca
b.well	BIDMC (Beth Israel Deaconness Medical Center)
Cambia Health Solutions	California
DirectTrust	CNSI
DrFirst.com	Merck
EMR Direct	Northeastern
Graphite Health	Pfizer
HHS XMS	UC Davis
ID.me	State of Utah
Intermountain	
iShare Medical	
Kantara	
Login.gov	
Massachusetts Health Data Consortium	
Mastercard	
Patient Centric Solutions	
Premera Blue Cross	
Providence Health Systems	
Optum Health / UnitedHealthcare	
ZenKey	

How Interested Participants Can Prepare

- **Consumer-facing Applications:** Ensure you are partnered with a CSP that issues IAL2 digital credentials and are certified by DirectTrust or the Kantara Initiative
- **Health Plans, Providers, EHR systems:** Will you use a CSP or will you be a relying party or both? Do you have a CSP solution that is part of or separate from your core system?
- **Credential Service Provider (CSPs):** Get certified with the Kantara Initiative or DirectTrust
- **Relying Parties:** What questions do you need to get answered internally before you can participate in the proof of concept and trust a digital identity coming from outside your organization?
- **Trust Framework Organizations:** Participate on our tiger team

Next Steps

1. Finalize the CARIN Digital Federated Credential Policy which provides policy equivalency across credential service providers.

2. Hold a proof-of-concept kickoff meeting in early December (Date still TBD) with interested participants (will involve CARIN and non-CARIN members).

3. Document the time and resource commitment, use cases, workflows, and success criteria for each proof-of-concept participant and gain commitments from those who have the resources to participate

4. Develop a feedback loop with policy makers and other interested parties (e.g., ONC, CMS, RCE, HL7, FAST, Public at large, etc.) and publicly document our proof-of-concept findings to engage the health care ecosystem at large

CARIN Workgroup Updates

CARIN HL7® FHIR® IG Related Workgroups

Implementation Guide	Purpose	Latest Updates	IG Page
CARIN IG for Blue Button® STU1 and STU2 (Health Plan WG)	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 a number of clients and servers successfully connected and exchanged the oral and vision types for the first time. Implementers also successfully tested at the November CARIN testing event. We will also test at the January HL7 Connectathon.	http://hl7.org/fhir/us/carin-bb/
CARIN IG for Digital Insurance Card STU1 (Health Plan WG)	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.	https://build.fhir.org/ig/HL7/carin-digital-insurance-card/
CARIN IG for Consumer-facing Real-time Pharmacy Benefit Check STU1 (RTPBC WG)	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.	http://hl7.org/fhir/us/carin-rtpbc/

Additional Workgroups

- **Trust Framework and Code of Conduct**
  - CARIN Code of Conduct: https://bit.ly/CARINCodeofConduct
  - CARIN App Registration Guide: https://bit.ly/CARINAppRegistration
  - CARIN UX Guide: Home | CARIN UX Guide (arcwebtech.com)
  - Ongoing work to advance CARIN Code of Conduct with various industry certification organizations
  - Ongoing discussions with VHA, CCIIO, & CMS about developing a common public sector application registration process
  - Ongoing discussions with Graphite Health about implementing CARIN application registration and digital identity best practice concepts in order to develop common private sector processes

- **Digital Identity and Consent**
  - Proof of Concept with HHS
    - ID proofing and Authentication *across* providers, health plans, and consumer-facing applications
  - Operationalize the digital identity federation credentialing policy across trust framework organizations
  - Working with ONC FAST on consent and matching

- **Policy**
  - Comments to CMS, ONC, RCE
  - Meetings with HELP, E&C, CMS, ONC, OCR, RCE

BREAK

SMART Health Cards

Opportunities to Collaborate

Smart on Value

LEAVITT PARTNERS

@carinalliance | www.carinalliance.com | HL7.org/CARIN

801-538-5082

www.leavittpartners.com

@LeavittPartners