Digital Identity Federation in Health Care | The CARIN Alliance and Department of HHS Digital Identity Proof of Concept

Tuesday April 18, 2023

HIMSS 23

DISCLAIMER: The views and opinions expressed in this presentation are solely those of the author/presenter and do not necessarily represent any policy or position of HIMSS.

Meet Our Speakers

Ryan Howells
Leavitt Partners
Principal

Blake Hall
ID.me
Chief Executive Officer

Bo Holland
AllClear ID
Founder & Chief Executive Officer

Darren Mann
Intermountain Healthcare
Interoperability Engineering Director

David Barden
CLEAR
General Manager, Head of Healthcare

Julie Maas
EMR Direct
Founder & Chief Executive Officer

Kyle Neuman
DirectTrust
Director of Trust Framework Development

Max Templeton
Cambia Health Solutions
Principal Architect

How to Learn More:

Digital Identity Federation Report

Digital Identity Federation Demos

The CARIN Alliance

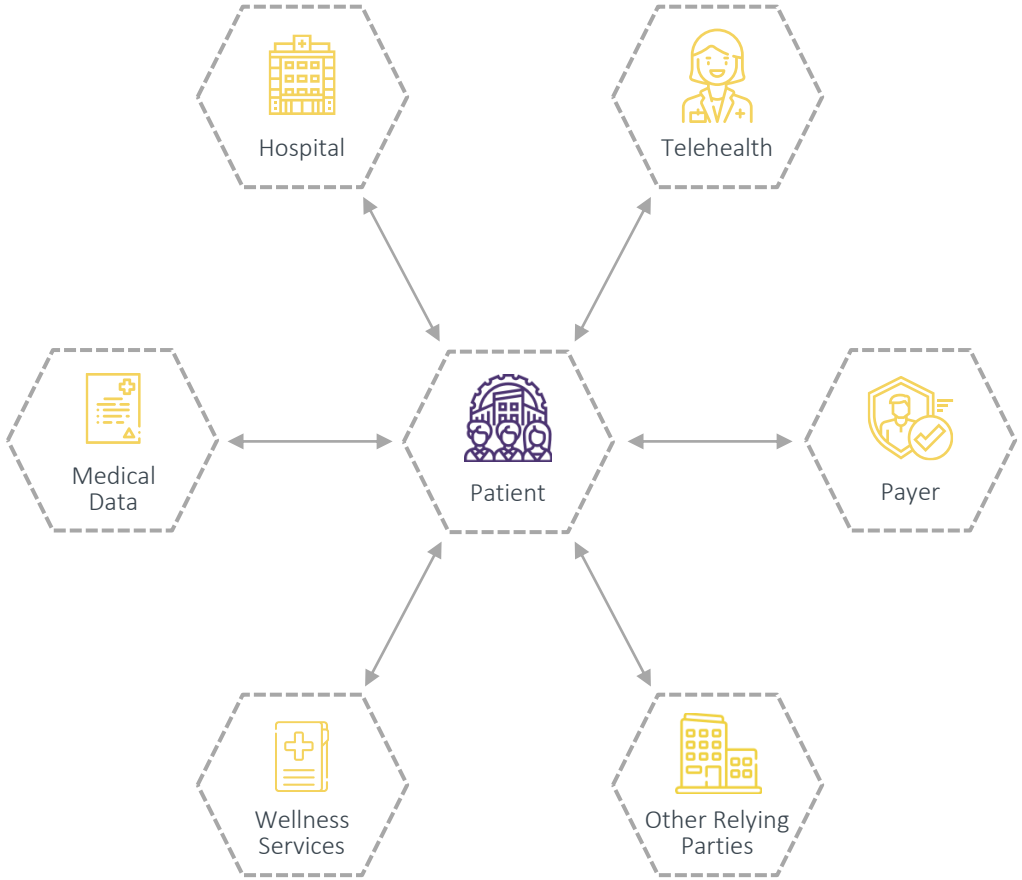
Our Vision

To rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health informatic when, where, and hov 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/

The Current State

A Person-Centric Approach to Health Data



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

Engage in telehealth or renew prescriptions with a physician virtually

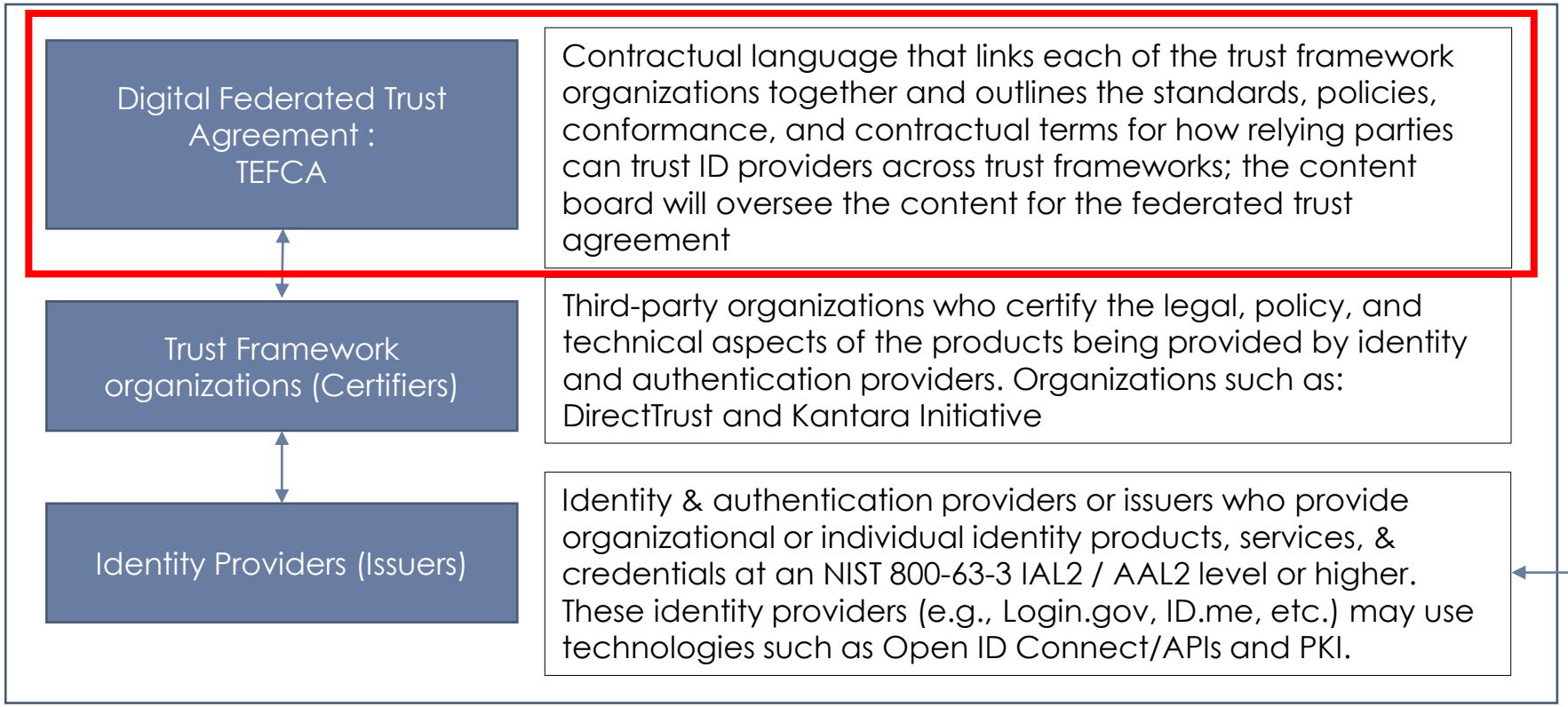
Obtain and exchange health information with HDOs, payers, health management apps and other business a patient chooses to engage with

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 healthcare related software systems

Interact with other relying parties that may not be involved in healthcare but are willing to consume identity assertions from healthcare-oriented identity providers

Federation and Trust: The Need to Create Policy Equivalency Across Trust Framework Organizations



Focus is on policy equivalency across technologies and trust frameworks (NIST 800-53, 800-63-3, RFC 3647)

Relying Parties

Anyone who wants to accept an IAL2 certified credential from an identity provider who has been certified by a trust framework organization

To access the Digital ID and Federation Whitepaper and the CARIN Credential Policy, go to:
CARINAlliance.com and select Our Work → Digital Identity → Download our Digital Identity and Federation White Paper and CARIN Credential Policy

How 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 is harmed 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?

CARIN / TEFCA Digital Identity Timeline

- **August 2017** : We first recommended to ONC they adopt the NIST 800-63-3 IAL2 guidelines
- **January 2018, April 2019, and January 2022** : First, Second, and Final versions of TEFCA recommended the adoption of a NIST 800-63-3 IAL2 digital credential
- **June 2019** : CARIN Digital Identity Summit in DC
- **December 2020** : CARIN released our whitepaper discussing how we could implement digital identity federation
- **January 2022 :** CARIN launched the Healthcare Digital Identity Federation PoC with HHS, CMS, and ONC
- **June 2022** : The IAS Exchange Purpose Implementation SOP recommended the approach we discussed in our 2020 whitepaper
- **July 2022** : CARIN commented on changes to the IAS Exchange Purpose SOP
- **September 2022** : The final IAS Exchange Purpose Implementation SOP incorporated the changes CARIN recommended in July and mandated a response from TEFCA network participants when an IAS provider follows the IAS SOP
- **March 2023** : **CARIN published the PoC Report and CARIN Credential Policy**

To access the Healthcare Digital Identity Federation Proof of Concept Report, go to:
CARINAlliance.com and select Our Work → Digital Identity → Download our Proof of Concept Final Report

CARIN / HHS Healthcare Digital Identity Federation PoC – Our 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 2021CARIN Community meeting: https://www.carinalliance.com/events/carin-community-meetings/

ROLE	ORGANIZATIONS
Application	b.Well Invitae MaxMD Otis Health Patient Centric Solutions
Credential Service Provider	1Kosmos – API (Full Service) AllClear ID – API (Full Service – In process) CLEAR – API (Full Service – In process) EMR Direct – PKI and API (Full Service) ID.me – API (Full Service) Persona – API (Full Service – In process) LexisNexis – API (Component) MaxMD – PKI Mastercard – API (Component) Persona – API (Full Service – In process)
Health Information Exchange (HIE)	CRISP, Rochester RHIO, and others connected to the Invitae Cures Gateway
Certificate Issuer	EMR Direct (UDAP™ Tiered OAuth) MaxMD (UDAP™ Tiered OAuth)
Identity Broker	Department of Health and Human Services NextGen XMS team (HHS XMS)
Relying Party	Cambia Health Solutions (Health Plan) Cedars-Sinai Medical Center (Provider) CVS Health (Health Plan) Kaiser Permanente (Provider) Marshfield Clinic Health System (Provider and Health Plan) Providence Health System (Provider) Providers participating in HIEs connected to the Invitae Cures Gateway Providers participating in HL7® FHIR® exchange using EMR Direct Interoperability Engine
Trust Framework	DirectTrust Kantara Initiative
Government Observer	Centers for Medicare and Medicaid Services (CMS) The Office of National Coordinator for Health Information Technology (ONC)

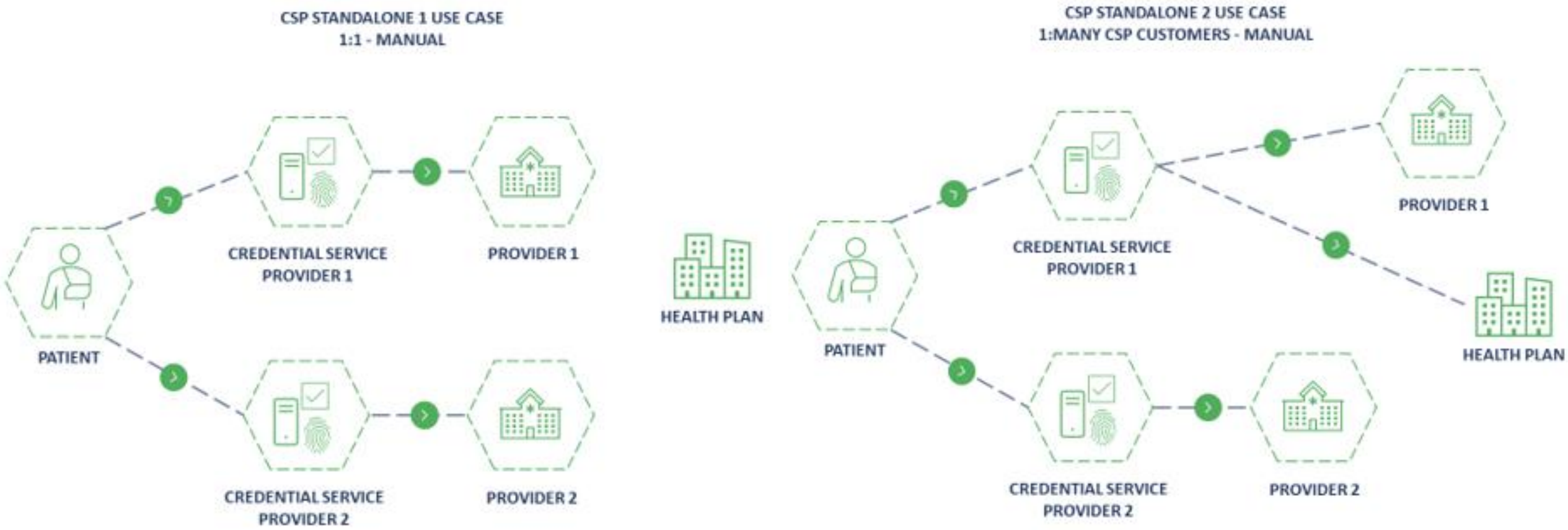
carin
Creating Access to Real-time Information Now through Consumer-Directed Exchange

Proof of Concept
Participants

CSP Standalone Use Cases, Objectives & Participants

Use Case(s)	Workgroup Objectives	Workgroup Participants
CSP Standalone / Interoperability (multiple Relying Parties) An individual user can authenticate and access their data from multiple relying parties.	• Integrate one of the CSPs into the data holder's system. • CSP will successfully identity proof *once* and authenticate an individual at IAL2/AAL2. • Portable IAL2 credential authenticates at AAL2 to multipleRPs (any integrated with the CSP).	• 1Kosmos • All Clear ID • Cedars-Sinai Medical Center • CLEAR • CVS Health • DirectTrust • EMR Direct • ID.me • Inpriva • Kaiser Permanente • LexisNexis • Mastercard • MaxMD • OtisHealth • Patient Centric Solutions

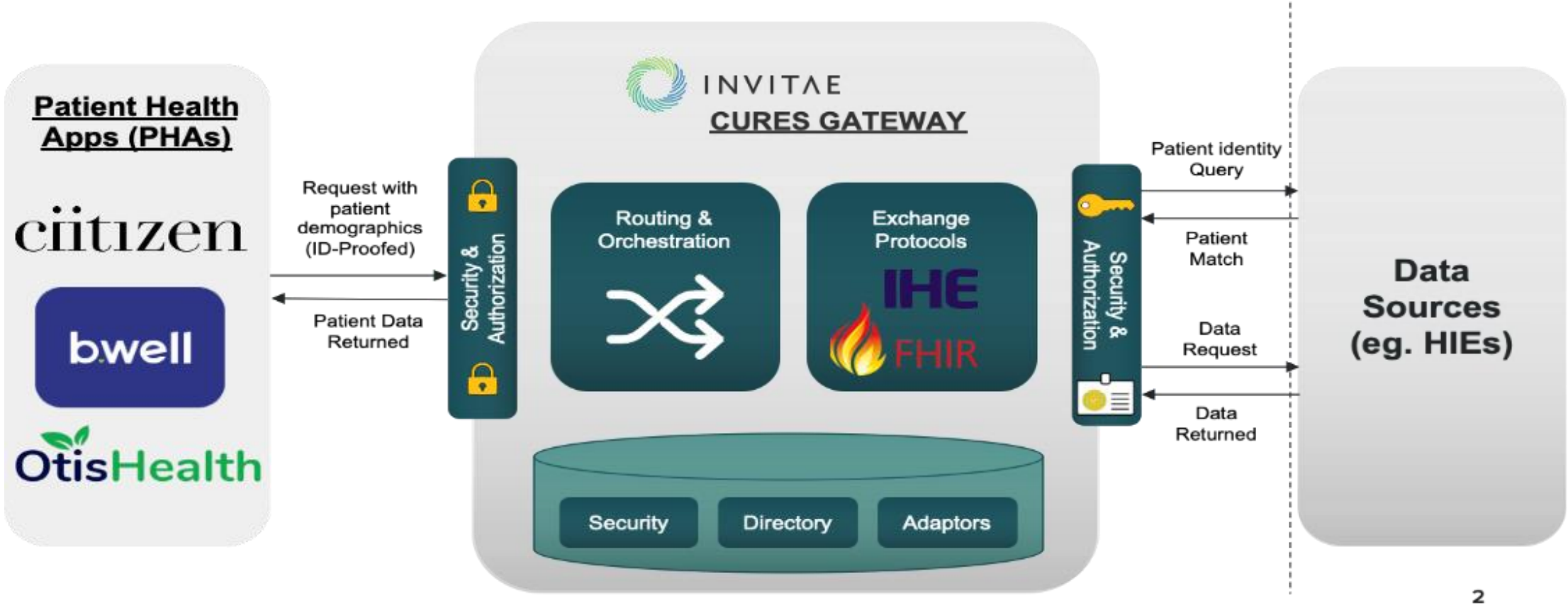
CSP Standalone Use Case Flows



CSPs with HIEs Use Case, Objectives & Participants

Use Case	Workgroup Objectives	Workgroup Participants
HIE Workflow (Non-FHIR APIs Flow) Involves agreeing to the policies associated with the specific HIE and passing the validated demographic information to query the HIE.	• Launch of Gateway (platform) that connects patient health apps (PHAs) to health information exchanges (HIEs). • Connected PHA identity proofs patients at IAL2/AAL2. • Connected PHAs send demographic queries through the Gateway to HIEs. • Gateway pushes queries and returns associated payload(s) from any connected HIE. • All Gateway participants sign binding agreements to abide by Gateway terms and conditions.	• b.well • Persona • OtisHealth • HIEs connected to the Invitae Cures Gateway

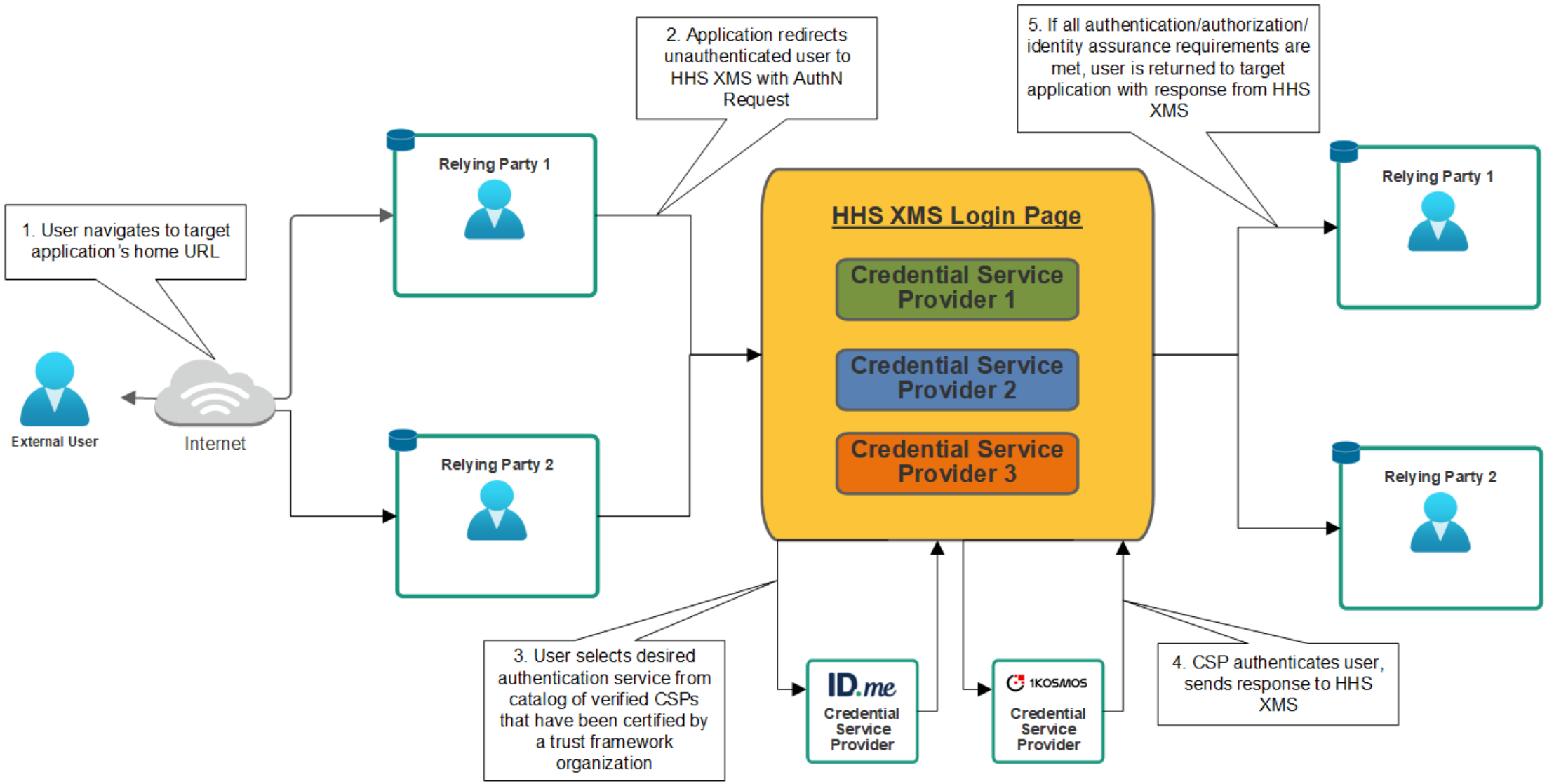
Cures Gateway Architecture



CSPs with HHS XMS Use Case, Objectives & Participants

Use Case	Workgroup Objectives	Workgroup Participants
HHS XMS (Multiple CSPs) A single individual can use one or more CSP credential to access integrated relying parties.	• Technically integrate HHS XMS into the portal or the app. • RP will successfully use one of the CSPs in HHS XMS to identity proof and authenticate the individual at IAL2/AAL2.	• HHS XMS* • Marshfield Clinic Systems* • Patient Centric Solutions* • 1Kosmos* • ID.me* • b.well • DirectTrust • Inpriva • Kaiser Permanente • MaxMD • Security Health Plan *Testing participants

HHS XMS Use Case Flow

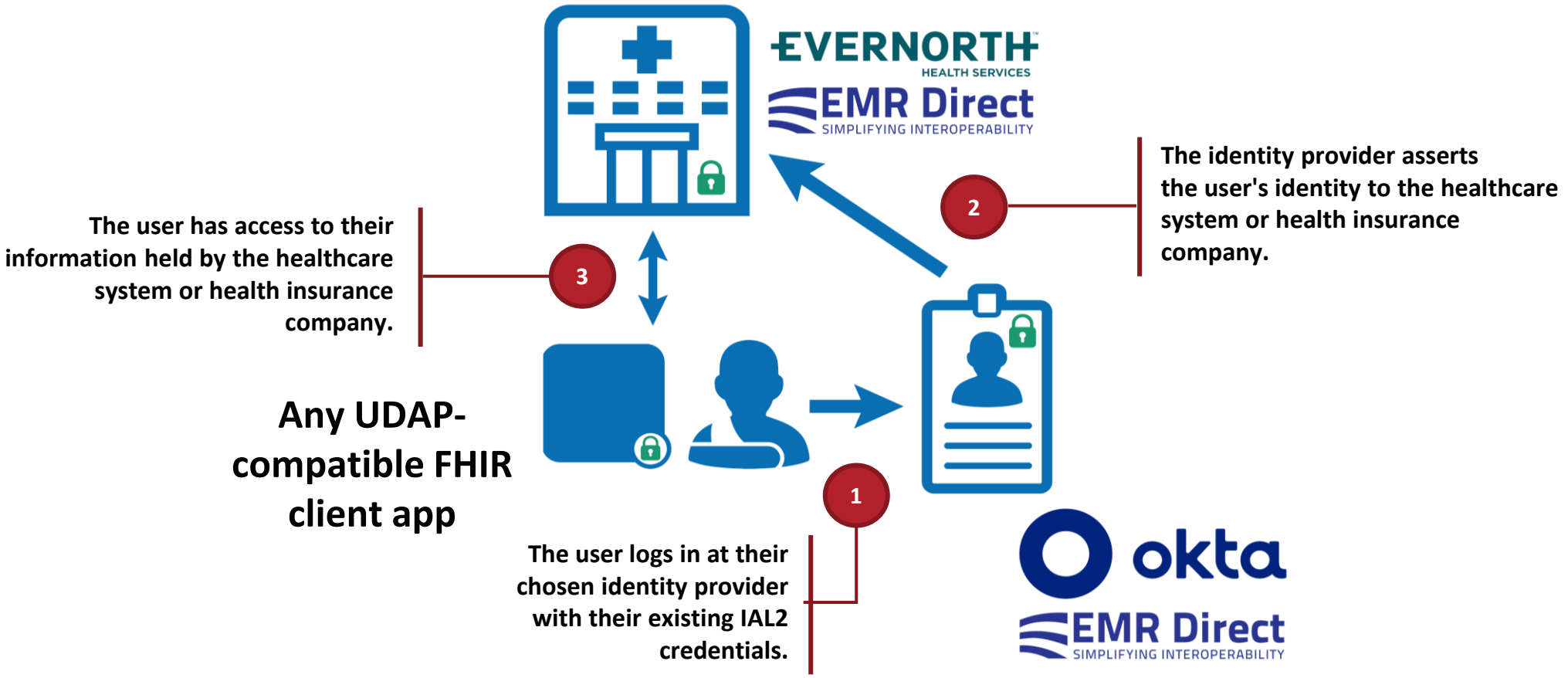


CSPs with UDAP Tiered OAuth Use Case, Objectives & Participants

Use Case	Workgroup Objectives	Workgroup Participants
CSP with UDAP (HL7® FHIR® Network Transactions) A data holder releases data to a "User Client App" as directed and authorized by a user (authenticated user data goes directly from CSP to RP). This is an HL7® UDAP Security & HL7® FAST Identity flow.	• All parties independently adopt the public UDAP Tiered OAuth or B2B standard. • CSP (or Client App in the case of UDAP B2B) successfully identity proofs and authenticates an individual at IAL2/AAL2. • RP and Client App will successfully use UDAP Tiered OAuth for User Authentication. User's credential with the CSP is automatically reusable with any other Client & RP that have implemented UDAP Tiered OAuth & trust the CSP -**OR-** Client passes assertions about the user's identity in an Authorization Extension Object per UDAP B2B.	• 1Kosmos • B.well • Cedars-Sinai Medical Center • EMR Direct • Evernorth • Okta • OtisHealth

UDAP Tiered OAuth

The user wishes to access their data held by a system where they don't have credentials. They specify an approved identity provider for authentication.

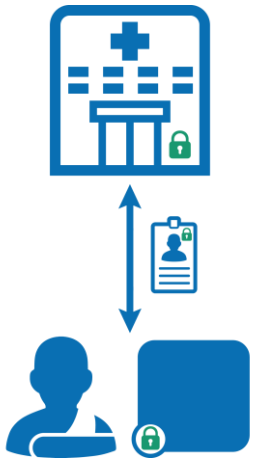


Interoperable Digital Identity & Patient Matching

We prioritized patient-facing (B2C) and payer/provider (B2B) interaction as focus areas.

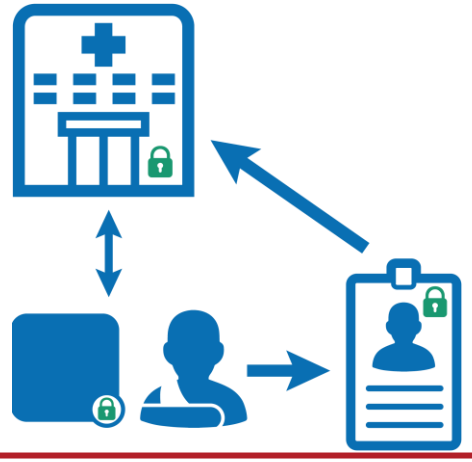
Trusted Identity Services provide user authentication, and unique identifiers for matching or other verified demographic data, all meeting best practice match input & minimum verification level floors.

App-Mediated Business-to-Business with Patient User



Networked Identity Management:

- **Patient-Mediated Business-to-Consumer,**
- **Patient-Directed Business-to-Consumer**



Includes Patient-facing workflows IAL1.8/AAL2 Focus on identity management

Best practice-compliant probabilistic matching services use demographic data from health data requestor and unique identifiers when possible. Requestor follows match input floor & minimum identity verification.

Mediated Patient Matching: Business-to-Business

- **Coverage,**
- **TPO, or**
- **Patient Request**

Payer/Provider interactions IAL1.5 Focus on best practice patient matching

Connectathon Track Page:
2023 – 05 FAST Infrastructure (Security, Identity, Directory, Exchange)

Implementation Guide:
Interoperable Digital Identity & Patient Matching (CI Build)

HL7 Milestone *(May 2022 Ballot Cycle)*	Due Date
Project Proposal	✓
Project Scope Statement (PSS)	✓
FHIR IG Proposal	✓
Notice of Intent to Ballot (NIB)	✓
Ballot reconciliation	✓
Publish STU 1	April 2023

UDAP and the green lock and ecosystem gears designs are trademarks of UDAP.org and are used with permission.

Lessons Learned and Future Considerations

Patient Considerations

- Involve patient users and other constituents in evaluating the use cases and participation levels to help fine tune next steps.
- Continue the conversation about the various actors involved in these data access use cases, as well as their discovery and trustworthiness, especially where patient privacy and individually identifiable data and health data are concerned.
- Employ fictional test users and test data at the beginning of the experiment that is based on the ONC EHR Test Data.
- Establish an OIDC assertion profile that implements and/or extends OpenID Connect Core Standard Claims from section 5.1.
- Convey any new feedback about essential demographic attributes that each data holder uses to match patients to help establish consensus on a set of attributes that will be included in every assertion. The attributes might include unique identifiers such as driver's license numbers, passport numbers, and HL7 Digital Identifiers as well as last 4 of SSN, mobile phone number, email address, and other attributes.
- Encourage CSPs to establish processes for collecting and validating attributes that are essential to health information exchange during the ID proofing process.
- Include processes and profiles for CSPs to include historic addresses within the assertions sent to data holders because the data holder may have stale data pertaining to a patient's previous address and may fail to match if the CSP only asserts the most recent patient address.

Lessons Learned and Future Considerations

CSP Interoperability and Functional Testing

- When testing automated or dynamic federation across multiple CSPs and relying parties, ensure the test case has at least two CSP participants and at least two relying party participants to adequately test the interoperation between all parties at scale.
- When testing automated or dynamic federation across multiple CSPs and relying parties, produce open source test data and a test infrastructure at the beginning of the experiment to allow any party to test in a uniform and uninhibited manner.

Financial Considerations

- Research mechanisms that allow for different financial models to be employed. Some models may allow a relying party and CSP to dynamically arrive at a per-transaction fee and exchange payment. Others may charge one party a monthly or annual cost for managing a credential and allow that credential to be used anywhere that will accept and trust it, at no additional charge. Additional financial models may prove to be viable.

Lessons Learned and Future Considerations

Legal Considerations

- Involve each relying parties' legal team from the beginning, in a tangential role. This allows the legal team to observe the technical and business relationships that are tested and conceptualize the liability risks that such relationships may create. These observations and mitigating language can be incorporated into a policy document such as the CARIN Credential Policy.

Cybersecurity and Risk Management Considerations

- Involve the CISO and risk management teams of the relying parties at the beginning of the experiment. Such an approach allows the cybersecurity team to observe the technical and business relationships that are tested and conceptualize the risks that such relationships may impose on the organizations they serve. These observations and mitigations can be incorporated into a policy document such as the CARIN Credential Policy.

Future Paths Toward Federation

Based on this proof of concept, there are two preferred paths toward digital identity federation:

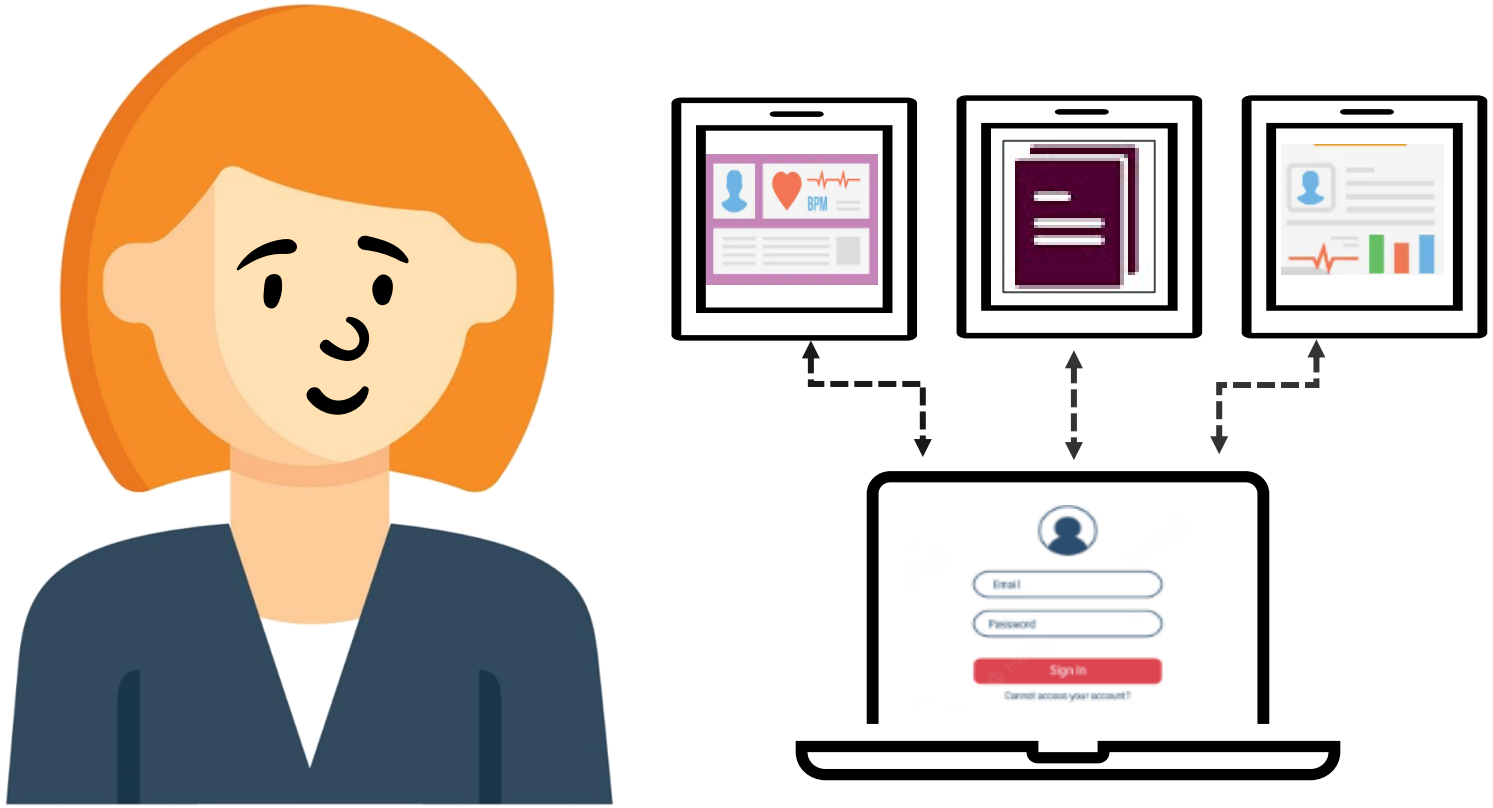
1. Leveraging HHS XMS as a national identity broker service

HHS XMS provides an opportunity to ensure trust in brokering digital identities across the health care ecosystem with both public and private stakeholders. XMS could act as a 'Single Sign On'-like service that is vendor agnostic so individual health systems, payers, and applications can add the XMS widget/service to their website thus enabling individuals to execute a 'Log In With' scenario from a CSP of their choice. We look forward to working with HHS, ONC, and CMS on the next steps related to this opportunity.

2. Leveraging the UDAP™ Tiered OAuth Protocol

As outlined in the HL7® UDAP™ Tiered OAuth implementation guide, there is an opportunity to leverage this protocol across the health care ecosystem as a means by which secure digital identities can be leveraged by relying parties. Organizations who do not currently have a relationship with each other can use a combination of the technological functionality provided by the protocol along with the trust framework components previously mentioned in this report.

The Future State



Questions?

Contact Information

Ryan Howells, MHA, PMP

Principal, Leavitt Partners

Program Manager, CARIN Alliance

Twitter: @RRyanHowells

LinkedIn: https://www.linkedin.com/in/ryanhowells

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