LEAVITT PARTNERS
An HMA Company

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

Healthcare Digital Identity Federation Proof of Concept Report

March 2023

The CARIN Alliance and **U.S. Department of Health and Human Services**

Table of Contents

Executive Summary 2
Objective 3
Participants 3
Scope 3
Meeting Cadence 3
Partnerships 3
Standards 3
NIST 800-63-3 IAL2 Requirements 4
Using IAL2 and AAL2 for Identity Proofing 5
Trust Framework Approach and the CARIN Credential Policy 7
The Problem 7
A Person-Centric and Trust Framework Approach Using the CARIN Credential Policy 7
Test Data Attributes Used for the Workstreams 9
Workgroups and Report Outs 10
1. Use Case #1 – CSP Standalone 12
2. Use Case #2 – Health Information Exchange 17
3. Use Case #3 – HHS NextGen External User Management System (XMS) 21
4. Use Case #4 – CSP with UDAP™ Tiered OAuth 30
Conclusions 35
Preferred Paths Toward Federation 36
Recommendations and Lessons Learned for Future Testing 36
Areas for Future Engagement 37
Appendices 39
Appendix A. Master Participant List 39
Appendix B. Acronym Table 40
Appendix C. Definitions Adopted and Used for the Proof of Concept (PoC) 41
Appendix D. Additional Definitions of Interest to the PoC 45
Appendix E. Crosswalk of ONC, OIDC, USCDI Data Elements with FAST Patient Weighted Input 47
Appendix F. HHS XMS Technical Flows (OIDC and SAML 2.0) 50
Appendix G. Initial Minor's Identity and Personal Representative's Use Cases 52

Executive Summary

Passage of the 21st Century Cures Act, the Office of the National Coordinator for Health Information Technology (ONC) Cures Act Final Rule, and the Centers for Medicare & Medicaid Services (CMS) Interoperability and Patient Access rule have accelerated individuals' ability to access their personal health information via an application of their choice, including leveraging Health Level Seven International (HL7®) Fast Healthcare Interoperability Resources (FHIR®) Application Programming Interfaces (APIs). At present, SMART on FHIR® allows individuals to use their provider or payer portal usernames and passwords to authenticate themselves and retrieve their personal health information.

The CARIN Alliance endorses the current implementation of SMART on FHIR® by stakeholders in the healthcare ecosystem to ensure individuals have immediate access to their health information; however, we also seek to advance a future vision for how individuals can voluntarily digital identity proof themselves in a trusted way without the need to create separate portal accounts with every data holder who currently holds their health information. Individuals seeking their health information could then use that same trusted identity proofed digital credential to access their health information across multiple payers and providers.

Consequently, the CARIN Alliance, the Department of Health and Human Services (HHS) NextGen External User Management System (XMS) team, the Office of the National Coordinator for Health Information Technology (ONC), and the Centers for Medicare and Medicaid Services (CMS), partnered to lead a public/private sector effort to develop a digital identity federation Proof of Concept (PoC). The PoC's objective was to scale an open framework for federating trusted NIST 800-63-3 Identity Assurance Level 2 (IAL2) certified credentials using a person-centric approach across healthcare organizations, leveraging modern technologies such as OpenID Connect and OAuth 2.0. Participants in the PoC, which included applications, credential service providers (CSPs), certificate issuers, identity brokers, government observers, relying parties (RPs), and trust frameworks, tested four use cases that varied in complexity and support related to their automation of trust.

The report details the scope and testing process of the four workgroups in the PoC: CSP Standalone, CSPs with Health Information Exchanges (HIEs), CSPs with the HHS External User Management System (XMS), and CSPs with the HL7® Unified Data Access Profiles (UDAP™) Tiered OAuth open protocol. This report enumerates lessons learned to foster future experiments and pilots related to digital identity and API-based health information exchange. The report includes suggestions for level-setting expectations at the start of the pilot and for involving the right stakeholders to participate or observe the pilot, as well as recommendations about which hypotheses to test in the future and how best to test those innovations. These recommendations are provided as a means to build on the work that has already occurred and define how the healthcare system can move toward an interoperable, equitable, resilient, and secure federated digital identity ecosystem in which trustworthy API-based exchange can be executed.

Objective

Our overall objective was to determine a set of feasible options for scaling an open-source framework to federate trusted NIST 800-63-3 Identity Assurance Level 2 (IAL2) certified credentials across healthcare organizations using a person-centric approach. Our focus was on using existing technology infrastructure that either has been or will be in place in U.S. healthcare based on recent ONC and CMS federal interoperability regulations that require providers and payers to use more modern technologies such as OpenID Connect and OAuth 2.0. Nascent technologies such as distributed ledger, decentralized identifiers (DIDs), and self-sovereign identity (SSI) were not considered primarily because the trusted, open standards and framework necessary to implement those nascent technologies, including a robust trust framework and more modern authentication standards, need to first be in place before moving, if ever, toward a more decentralized approach.

Participants

PoC participants included applications, credential service providers (CSPs), certificate issuers, identity brokers, relying parties (RPs), trust frameworks, and government observers. A list of participants is in Appendix A.

For the PoC, participants noted a difference between full-service and component CSPs as currently defined by Kantara Initiative. Full-service CSPs provide both identity proofing and authentication, whereas component CSPs provide just one of those capabilities. Both were considered CSPs for the purpose of the PoC, and the PoC determined that identification and authentication could be achieved through partnering with other component providers.

Scope

Meeting Cadence

The PoC met biweekly following the kickoff in March 2022. Beginning in August 2022, the PoC members decided to also split into four workgroups: CSP Standalone, CSPs with HIEs, CSPs with HHS XMS, and CSPs with UDAP™ Tiered OAuth. The workgroups met biweekly through the end of the year and are discussed in more detail below.

Partnerships

The PoC partnered with HHS to test its XMS identity broker service and the FAST digital identity and patient matching tiger team to test UDAP™ Tiered OAuth.

Standards

NIST-800-63-3, NIST SP 800-53rev5, RFC 3647, Open ID Connect (OIDC), SMART on FHIR/OAuth 2.0, UDAP™ Tiered OAuth, and other open standards guided the PoC.

The PoC also provided a use case background that informed the development of the CARIN Credential Policy,[1] which outlines the technical, policy, legal, and certification guidelines necessary to create trust so

[1] The CARIN Credential Policy can be accessed on the CARIN Alliance website at https://www.carinalliance.com/our-work/digitalidentity/.

digital identity credentials can be used and accepted even when issued and certified by different credentialing providers and trust framework organizations.

NIST 800-63-3 IAL2 Requirements

When the PoC started, the National Institute of Standards and Technology (NIST) Digital Identity Guidelines included a self-asserted no-assurance tier (IAL1), a high-assurance tier (IAL2), and a very high-assurance tier (IAL3), which, in general, only the federal government uses. IAL2 was the primary assurance level for online, remote identity proofing. Hence, the Trusted Exchange Framework and Common Agreement (TEFCA) draft language identified IAL2 as the baseline for all TEFCA users, including patient users of individual access services (IAS). During the PoC, NIST came out with 800-63 Revision 4 for public comment, but given that it came out during the PoC and the comment period, finalization, and certification infrastructure necessary to support it are likely years away, the group did not include Revision 4 as part of the PoC. Based on increasing levels of adoption, the PoC members saw value in the identity assurance resulting from an automated comparison of a real-time selfie to a government-issued photo identification (ID) number — a core component of IAL2 remote. For all of these reasons, the PoC members focused on NIST 800-63-3 IAL2 requirements for identity proofing purposes. The PoC members are closely watching the development of the next revision of the NIST Digital Identity Guidelines to see how changes will impact patient access and other use cases.

Participants considered the following benefits and drawbacks of IAL2:

Benefits

- Increased identity assurance for the end user in IAS use cases beyond what is currently required of data holders in today's environment, which is crucial to access data via national networks.
- As such, IAL2 may ease the ability for relying parties to approve the federation of identity credentials.

Drawbacks

- The end user or proofing solution must provide identity evidence to attain IAL2. Current implementation of this evidence collection has been automated for most but not all population segments (e.g., minors, people experiencing housing insecurity, etc.). Solutions exist to help these individuals attain IAL2 via video chat or an in-person visit at a brick-and-mortar location. While these alternative pathways maximize coverage across demographics, segments of the population still face systemic challenges, including lack of broadband internet access or personal preferences, such as not wanting to participate in a video chat, which may necessitate non-digital channels to attain 100 percent coverage.
- The volume of evidence to attain IAL2 is higher than most individuals are accustomed to (e.g., identity proofing versus basic registration information), but given the sensitivity of user health information, an opportunity to educate the market on the importance of portable, high assurance digital identity is evident.
- When conducting experiments such as this PoC, identity proofing cannot be tested with test users. This type of activity would require the use of forged or fake identity documents; therefore, the actual process for attaining an IAL2 credential was not tested in the PoC. However, the actors (CSPs) that performed the ID proofing functionality were expected to have or be in pursuit of an IAL2

accreditation from a third-party accreditation body such as DirectTrust or the Kantara Initiative and so PoC members had confidence in the fact the identity proofing activity was executed in accordance with the NIST guidelines.

Though the PoC decided to require IAL2, the PoC also discussed whether a lesser IAL level could be accepted. The HL7® FAST Identity team has introduced recommended levels, which are between IAL1 and IAL2, for public comment within HL7®. A working draft of these levels can be viewed here. These levels as drafted are intended to reflect some of the differing levels of identity verification in practice today, which generally include the following components:[2]

- Declaration: A declaration of identity assertion is required starting with IAL1 and continues to IAL2, with the associated requirements getting stronger as the levels progress.
- Identification: The evidence requirements vary when progressing to increased levels of identity assurance and there are sometimes differences in the requirements for remote versus in person verification.
- Notice: When notice is required, some levels permit notice to be mailed to a home address, or if the individual has supplied a verified email, to the email address.

Participants noted that in their current practice, most fall within the HL7® IAL1.5 to 1.6 range.

One of the changes NIST is considering in the updates to NIST 800-63 would adjust IAL2 by removing the requirement for a second fair piece of evidence when a strong photo ID is used. Draft language about moving IAL1 away from simple self-assertion by including some level of identity verification is under consideration. These additions, if finalized, may prove helpful by offering an intermediate identity assurance option for industry to explore that impacts fraud prevention and customer experience.

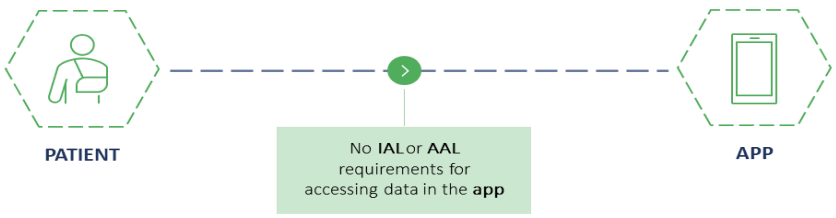
Using IAL2 and AAL2 for Identity Proofing

The three scenarios, below, describe when IAL2 and AAL2 requirements come into play.

Scenario 1: Direct Access to Application Data

In this scenario depicting the direct interaction between an application and the patient, the patient and the app vendor can agree directly on the level of identity proofing (IAL) and authentication (AAL) required because the transaction is specific only to those two actors. This means that identity proofing or authentication requirements for interactions between the application and the patient for access to data already present in the application are not inherent. See Figure 1 for this interaction.

Figure 1. Example of Direct Access to App Data

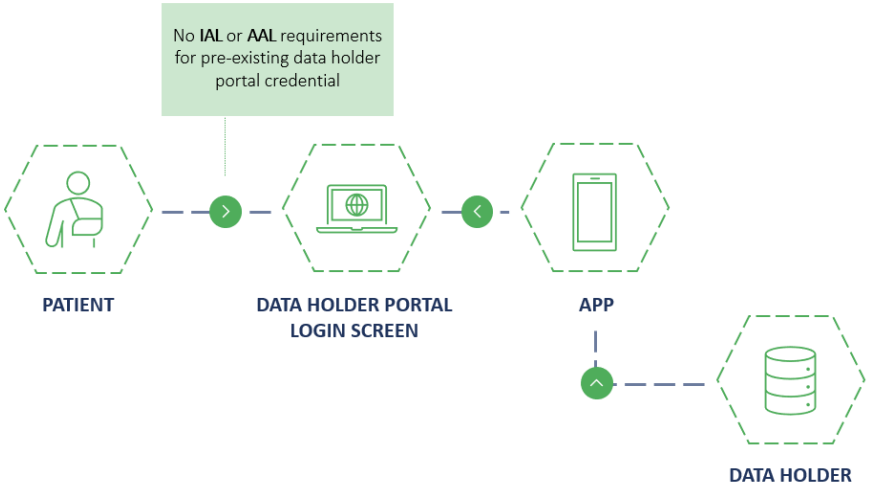


[2] The interim levels and the HL7® Identity Implementation Guide (IG) are intended to be consistent with NIST 800-63 except where specifically indicated otherwise. Future versions of these documents are expected to align with version 800-63-4 as that content is finalized.

Scenario 2: Authentication with the Data Holder Using Data Holder Credentials

Another scenario where identity proofing and authentication are not strictly relevant to the patient and application interactions is when a patient authenticates their identity to the data holder using credentials the data holder manages. In this scenario, the application is not asserting an identity externally. Rather, the application is "relaying" a login screen from the data holder to allow patients to authenticate themselves directly with the data holder (i.e., not using the credentials that patients established with the application). See Figure 2 below for this interaction.

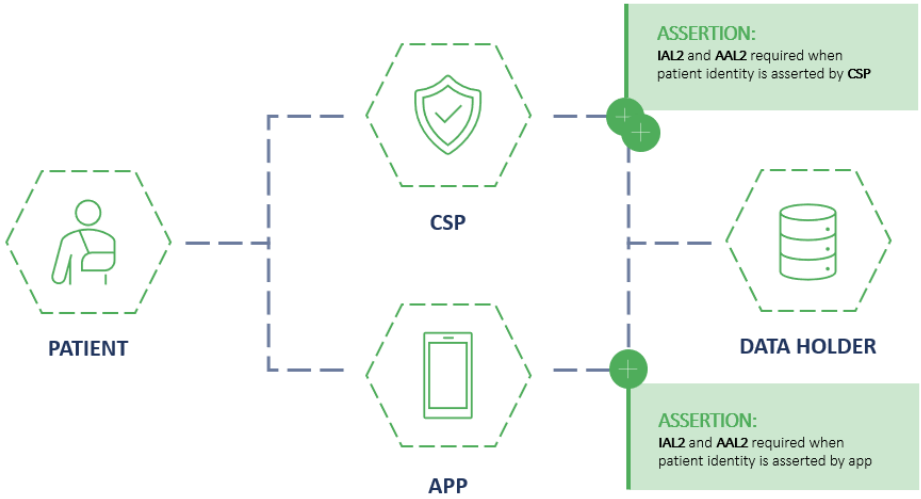
Figure 2. Example of Authentication Using Data Holder Credentials



Scenario 3: Asserting Identity Externally to Access Data

IAL and AAL requirements come into play when the application or CSP is asserting the identity externally to retrieve data from an outside source. In those scenarios, IAL2 and AAL2 should be observed to identity proof patients initially and to authenticate patients thereafter once their identity has been established before asserting their identity externally. See Figure 3 below for this interaction.

Figure 3. Example of External Identity Verification



Contrasting the first two scenarios with scenario three demonstrates the risk that should be mitigated. In the first two scenarios, patients prove their identity directly to the application or the data holder. No actor is asserting the patients' identity to another party. Once an actor asserts a patient's identity to an external party that is expected to trust the assertion, all parties must agree upon the common identity proofing and authentication standards, and the asserting party should be independently accredited. Otherwise, the parties do not have a tangible and dynamic way of building trust with one another. IAL and AAL help establish trust. This is also where trust frameworks come into play.

Trust Framework Approach and the CARIN Credential Policy

The Problem

Individuals cannot effectively aggregate their own health information because they need to prove their identity with each organization they have a relationship with (multiple OAuth processes) and do not have effective means to manage their data. The hurdles healthcare faces when attempting to institute consumer-directed health data aggregation include:

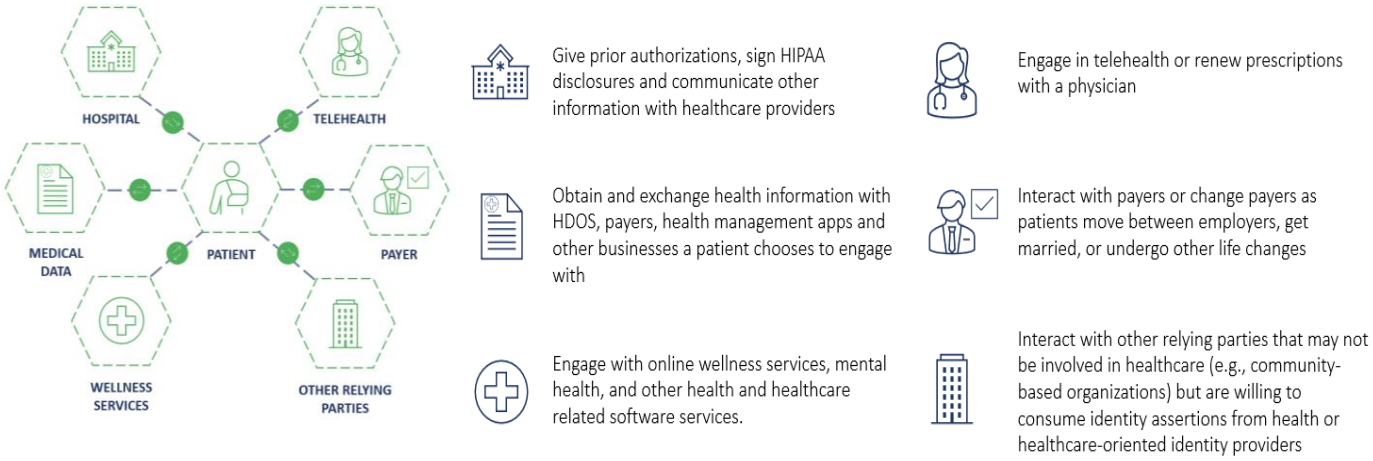
1. Scalable Trust: Scalable and convenient digital identity that can be used across many data holders in a trustworthy and interoperable way.
2. Legal Implications: Consideration of the liability involved in relying on a third party CSP's attestation of another individual's identity.
3. Patient Matching (Identity Resolution): The ability to resolve the consumer's identity at the data holder (hospital, payer, etc.) among a large pool of users with similar demographics using only the information received from a CSP. The evidence often used to meet IAL2 ID proofing requirements is not necessarily the same information necessary to achieve identity resolution. As a result, CSPs may need to adjust their onboarding processes to include the collection of information that may not help with ID proofing, but is useful to data holders for identity resolution.

The PoC asserts a person-centric approach, through a federated trust framework environment, could help solve these problems.

A Person-Centric and Trust Framework Approach Using the CARIN Credential Policy

A person-centric approach to health data access would allow people to prove their identities once and be issued a credential that different systems can accept. However, a way to establish trust is needed so that the multiple relying parties (data holders) that did not perform the identity proofing on their own can trust the patient's identity. This is where a trust framework provides value. Federating trust creates a mechanism for a third party (external to the relying organization) to rely upon the identity asserted by an external third party in a way that is dynamic and automated but reliable.

Figure 4. A Person-Centered Approach to Health Data Exchange

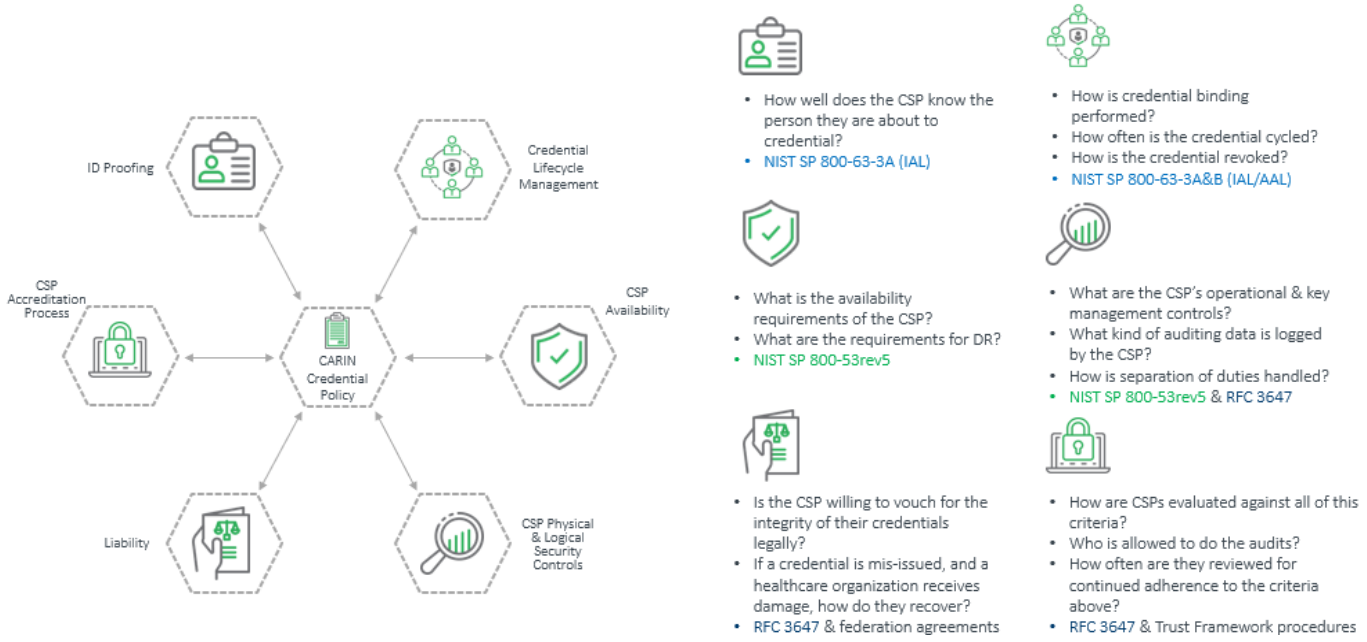


In the current point-to-point system, the relying party is responsible for evaluating every external third-party CSP to determine its trustworthiness in order to mitigate the relying party's risk. This is not scalable because it is expensive, time consuming, and unique to every relying party. Some relying parties may not have the necessary skill in-house to adequately evaluate CSP practices or foresee the legal implications of an agreement down the road. Consequently, the vetting of CSPs may be inadequate or the relying party may decide not to trust any external third party. For example, if the relying party does not require the external identity provider to assume liability for the identities it asserts, the relying party takes on all of the risk because that party is relying on the assertion with no way to recover if the CSP fails to properly manage or issue the identity. A point-to-point approach also increases the costs to CSPs because different relying parties will have different demands, rather than agreeing upon a common set of policies through consensus that all CSPs can subscribe to.

The need for a common set of policy requirements that all CSPs subscribe to served as the impetus for the CARIN Credential Policy. The Credential Policy was developed in collaboration with DirectTrust, Kantara Initiative, and the Electronic Health Network Accreditation Commission (EHNAC).[3] The intent was to create a policy that can be observed by all three accreditation bodies, who in turn, accredit CSPs. The CARIN Credential Policy offers the potential for policy equivalence across trust frameworks serving healthcare and potentially other industries, so a CSP accredited in one trust framework can be trusted by a relying party in another. The CARIN Credential Policy was developed in parallel to the CARIN PoC and was not observed by the CSPs participating in the PoC but was discussed and reviewed and serves as an opportunity for further study and consensus building around a common set of agreed upon CSP security requirements. Ultimately, the CARIN Credential Policy will become a public good. The CARIN Alliance is working with our public sector partners, including HHS, CMS, and ONC, to ensure the work we have done can be leveraged by all U.S. healthcare stakeholders. For more information and background on the CARIN Credential Policy, you can read our digital identity federation whitepaper on the CARIN Alliance website.

[3] On January 4, 2023, DirectTrust and EHNAC completed a merger of the two organizations, making EHNAC the accreditation arm of the DirectTrust Trust Framework and expanding DirectTrust's programs into consumer credentials and broader healthcare cybersecurity.

Figure 5. How Do We Determine Trust Across Credential Service Providers (CSPs)?



With a trust framework, all parties share liability in a way that is consistent with the responsibilities they accept as participants in the trust framework. Organizations that federate trust across multiple parties can scale this approach. In a trust framework, trust is determined by identity proofing, credential lifecycle management, CSP availability, CSP physical and logical security controls, liability, and CSP accreditation processes.

NIST defines baseline requirements that the parties can benchmark to associate the level of risk attributable to each type of participant. These criteria become the standards, and the trust framework determines the rules and policies implementing the standards and making them actionable. The trust frameworks will have a policy with a legal section that discusses the representations and warranties, dispute resolution mechanisms, how to proceed in the event of a catastrophic failure, limitations of liability, and other legal considerations to mitigate uncertainty.

The PoC used existing trust framework organizations, DirectTrust and Kantara Initiative, to federate trust and share liability across participating entities.

Test Data Attributes Used for the Workstreams

The PoC determined that, for most PoC workstreams, publicly available test data should be used for testing and related patient matching.[4] The PoC reviewed the patient matching attributes described in that section of the HL7® FHIR® Interoperable Digital Identity and Patient Matching Implementation Guide, the TEFCA Standard Operating Procedure (SOP): Individual Access Services (IAS) Exchange Purpose Implementation and United States Core Data for Interoperability (USCDI) v1. The HIE workstream tested using real patient

[4] Using publicly available test data prevents exposure of both identity/demographic information that may be used for matching (such as name, address, SSN Last 4) and health records themselves (the HL7® FHIR® health data resources a user is attempting to access in the various workstreams). It also allows flexibility to PoC participants since systems tested would not require the information security practices that production identity and health systems do.

data, with consent of those individuals, because it was testing a system expected to be fully launched in early 2023. References below to the "PoC" refer to the other three workstreams.

The PoC agreed on the list of attributes outlined in Table 1.

Table 1. Agreed Upon Attributes for Testing the POC Workstreams

SHALL Include	SHOULD Include
• First Name • Last Name • Date of Birth • Full current street address OR mobile phone OR email[5]	• Full current address (U.S. Postal Service) including City, State, ZIP • Mobile Phone • Email • When known, other patient demographic attributes within USCDI

The PoC reviewed several test patient sample data profiles generally supported by the test systems of certified Health Information Technology (Health IT), including electronic health records (EHRs) and profiles published by the Office of the National Coordinator for Health Information Technology (ONC). Because this is a testing environment, where the information would be available to anyone in the public, participants decided that the sample data would not include any protected health information (PHI), which would violate the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The group selected several test patients including Betsy Smith Johnson, Veronica Persinger, and Alice Newman. However, the PoC was unable to implement this test data before its conclusion. In support of future research, CSPs and EHR systems with the same users and demographics can use these pre-established test patients, allowing EHR systems to return a HL7® FHIR® bundle containing test health data for consumption by applications. Therefore, the PoC strongly recommends the use of test patient sample data as a minimum requirement for future experiments.

The PoC then developed a crosswalk showing what information is available at the intersection of ONC's test patients, the OIDC user profile, and required USCDI data elements, as well as how each of those items can be weighted to evaluate the expected success in single high confidence matching as identified in the HL7® FHIR® Interoperable Digital Identity and Patient Matching Implementation Guide. The group has yet to test the workstreams using the crosswalk but intends to do so in the future. The crosswalk can be found in the Appendix E.

Workgroups and Report Outs

The PoC tested four use cases/workstreams, organized below into the following corresponding workgroups. The use cases are organized from lowest to highest complexity and support for automation of trust. For example, the CSP Standalone use case requires each relying party to manually federate with each CSP to accept the CSP's identity. In contrast, the UDAP™ Tiered OAuth use case allows all parties that

[5] Participants in the PoC generally recognized that SSN Last 4 would also be a useful matching attribute, however it is not currently part of USCDI which is considered to be the starting point for demographic options enumerated in broad industry use. The HL7® FHIR® Interoperable Digital Identity and Patient Matching Implementation Guide emphasizes additional identifiers and recommends their use when available more broadly and (in some cases) after being included in USCDI.

support the UDAP™ Tiered OAuth protocol to trust each other dynamically with no manual configuration necessary to trust and accept assertions from a CSP after initial configuration of the protocol.

Table 2. PoC Workstreams

Use Case	Workgroup Objectives	Participants
CSP Standalone / Interoperability (1 or 2 Relying Parties) An individual user can authenticate and access data from multiple relying parties.	• Technically 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 multiple RPs (any integrated with CSP).	❖ 1Kosmos ❖ All Clear ID ❖ Cedars-Sinai Medical Center ❖ CLEAR ❖ DirectTrust ❖ EMR Direct ❖ ID.me ❖ Inpriva ❖ Kaiser Permanente ❖ Kantara Initiative ❖ LexisNexis ❖ Mastercard ❖ MaxMD ❖ OtisHealth ❖ Patient Centric Solutions
HIE Workflow (Non-FHIR® API 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 applications (PHAs) to health information exchanges (HIEs). • Connected PHAs identity proof 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.	❖ ID.me ❖ Ciitizen ❖ HIEs connected to the Invitae Cures Gateway ❖ Kantara Initiative ❖ Persona ❖ OtisHealth

HHS XMS (Multiple CSPs) A single individual can use one or more CSP credential(s) to access integrated relying parties.	• Technically integrate HHS XMS into the portal or the application. • Relying party will successfully use one of the CSPs in HHS XMS to identity proof and authenticate the individual at IAL2/AAL2.	❖ 1Kosmos ❖ b.well ❖ DirectTrust ❖ HHS XMS ❖ ID.me ❖ Kaiser Permanente ❖ Marshfield Clinic ❖ MaxMD ❖ Patient Centric Solutions ❖ Security Health Plan
CSP with UDAP™ (HL7® FHIR® Network Transactions) A data holder releases data to a "User Client Application" as directed and authorized by a user (authenticated user data goes directly from CSP to RP). This process is an HL7® UDAP Security & HL7® FAST Identity flow.	• All parties independently adopt the public UDAP™ Tiered OAuth or B2B standard. • CSP (or Client Application in the case of UDAP B2B) successfully identity proof and authenticate an individual at IAL2/AAL2. • The RP and Client Application 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

1. Use Case #1 – CSP Standalone

Today, patients and providers seeking access to health data are burdened with the requirement to manage separate user credentials for each system they log into. RPs must be able to trust a user's identity before providing data access. This use case exhibits the benefits for patients and providers and other stakeholders by simplifying that requirement yet maintaining the highest security.

- ❖ For patients, this means they can access their medical data across organizations integrated with the CSP with the same set of credentials.

- For RPs, this means they can trust a high-level authentication and know users are who they say they are, but also avoid onboarding the many users that need access.
- For the provider who often needs access to multiple clinical repositories, this means they can use the same set of credentials everywhere, following manual configuration of trust.

As we enable cross-facility interoperability, this use case will appear more than it does in the current state but is a necessity to enable our vision of healthcare interoperability. Figures 6 and 7 below demonstrate the two use cases this workgroup considered.

Figure 6. CSP Standalone Use Case 1.0

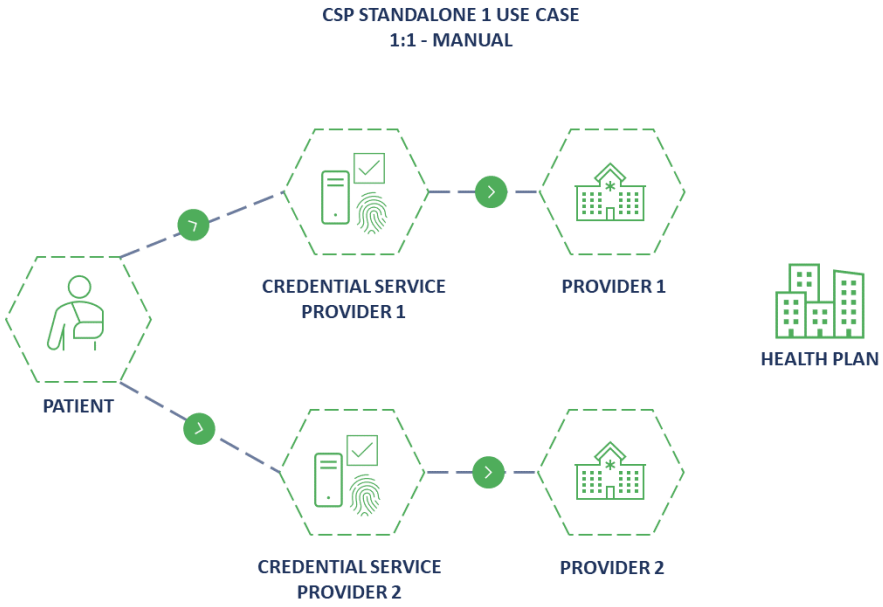
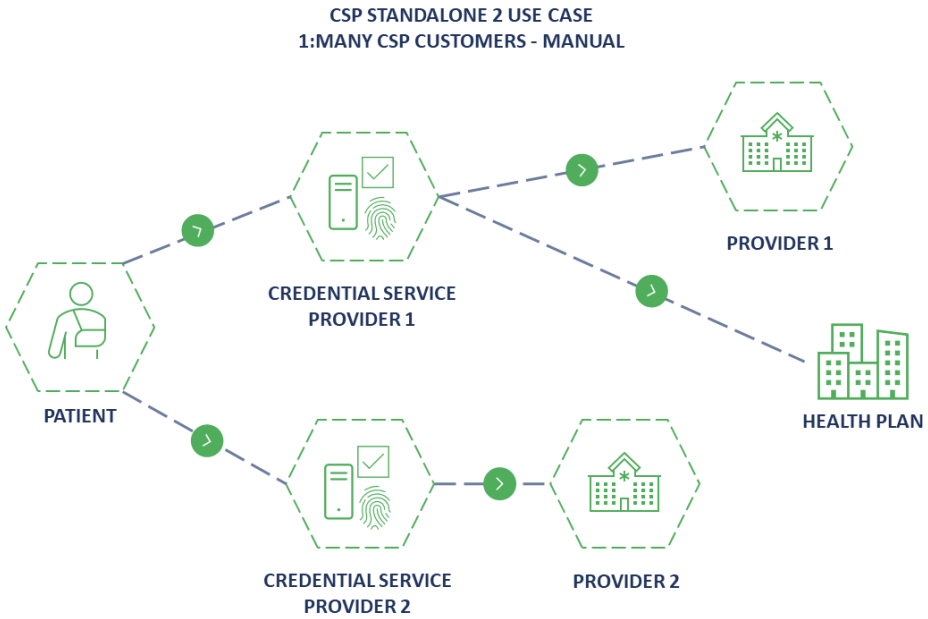


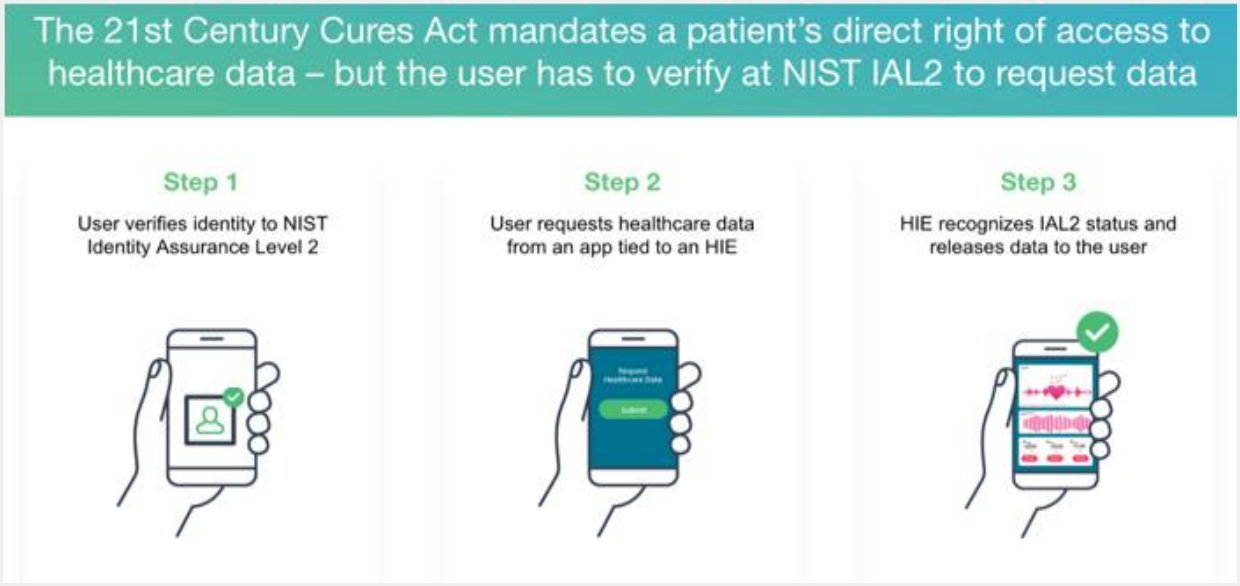
Figure 7. CSP Standalone Use Case 1.1



Testing Process and Final Report Out	
Description of User Journey	
Steps necessary for a CSP and an RP to trust one another and determine how (or if) they can do so dynamically	• CSP and RP establish a relationship. • CSP and RP agree on claims. • CSP and RP agree on assurance levels (IAL and AAL). • Configuration steps require manual configuration between the CSP and the RP. • RP provides CSP with a safe public Uniform Resource Identifier (URI) where CSP will redirect the user along with an authorization code. • RP provides CSP with a certificate to protect personally identifiable information (PII) during transit and the JSON payload is encrypted using Public Certificate Base64 value RSA 2048 bit. • CSP provides RP with authorization endpoint, token endpoint, attributes endpoint, client ID, client secret, and scope.
The user journey steps	• User chooses to access a resource through a client application. • User selects a CSP. • User selects an authenticator and binds the authenticator to their account at AAL2. • User conducts a one-time identity proofing event at NIST 800-63-3 IAL2. • User consents to share requested identity attributes information with the RP. • User is redirected back to the RP.
Pass through of ID-proofed user from first relying party to second relying party	• The first and second RP have an established relationship, data connection, security agreement, and privacy agreement which includes the IAL2 requirement for user authentication. • User selects to access a resource through a client application. • User selects a CSP. • User selects an authenticator and binds the authenticator to their account at AAL2. • User conducts a one-time identity proofing event at IAL2. • User consents to share requested identity attributes information with the RP. • User is redirected back to the RP. • User may now use the client application to select another RP from which to retrieve their health records.

	• The second RP receives authenticated user demographic information from the first RP and verifies a matching patient record. • Once the second RP finds a patient record matching the authenticated user, the user may retrieve their health records into the first RP client application.

User Experience



Participants in the Use Case
1. Credential Service Providers: 1Kosmos and ID.me 2. Relying Parties: Cedars-Sinai Medical Center, Kaiser Permanente, OtisHealth, and Patient Centric Solutions 3. Observers: All Clear ID, CLEAR, DirectTrust, EMR Direct, Kantara Initiative, Inpriva, Lexis Nexis, Mastercard, and MaxMD
How the Use Case Was Tested
• For the demonstration of this PoC, the team decided to only use test credentials. • The workgroup recorded videos of a pre-verified ID.me test user accessing their test environment. The video demos can be viewed on the CARIN Alliance YouTube page.
Test Data Used
• Test User Identity 1: ID.me leveraged the test user Veronica Persinger. The test user consented to share the following attributes with the RP: first name, last name, phone, street, city, state, postal code, birthdate, and email. • Test User Identity 2: Patient Centric Solutions tested with the Betsy Smith Johnson patient persona, which included the same attributes as the Veronica Persinger persona.   ○ The Betsy Smith Johnson persona is regularly used as a test user patient and has extensive clinical data. • Test User Identity 3: Patient Centric Solutions also leveraged a third test user, physician persona Dr. Erica, to show how she could access to her patient's data, using patient-mediated exchange.

Lessons Learned	

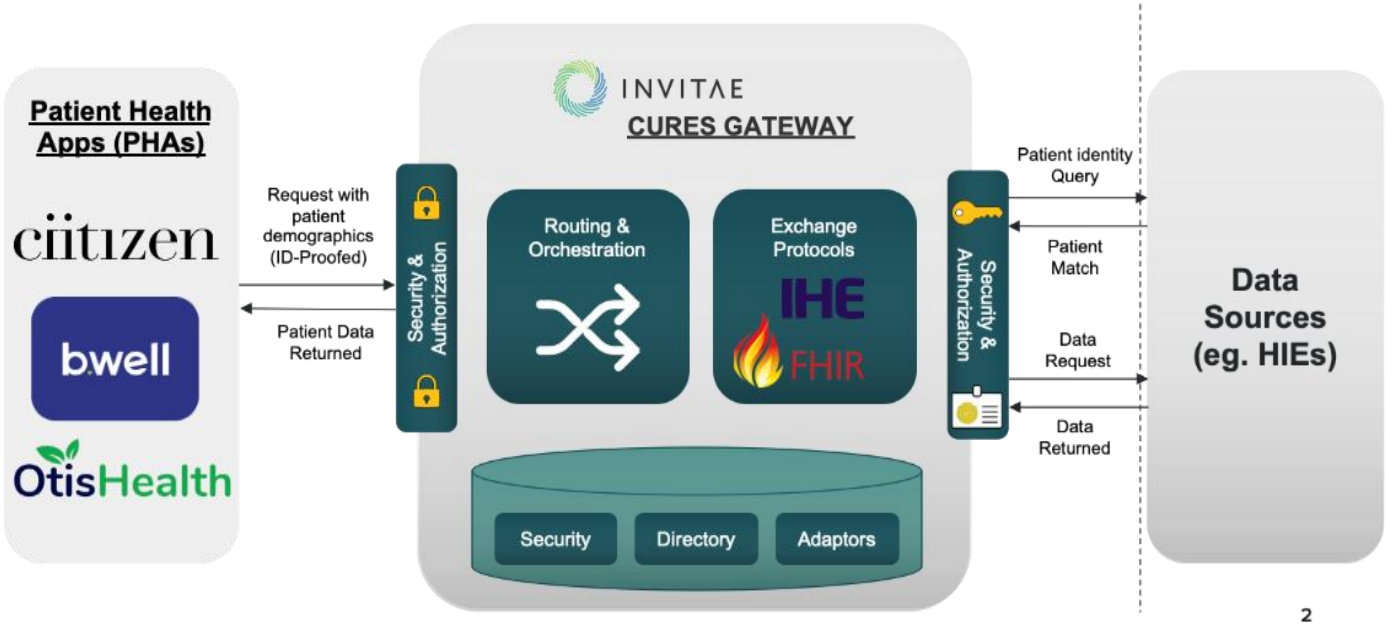
Benefits	• This process is easy to use and simplifies onboarding and user access.
	• Users can use one trusted credential to interact with multiple healthcare systems.
	• Healthcare systems have a high level of confidence and trust in the user's authentication because:
	  ○ Patients can access their own medical data in the healthcare repository, and the RP has increased confidence the patient is who they say they are and match the patient data they have on record.
	  ○ RPs can be assured that the clinicians accessing data are who they say they are.
	  ○ Secure clinical information exchange is increased.
	  ○ When coupled with consent, secure clinical information exchange can be automated.

	• This process enables patient matching based on secure, verified data.
How the industry can improve	• To date, major EHR vendors do not accept OIDC third party credentials; therefore, RPs leveraging those EHRs have difficulty incorporating a CSP into their environment. • Industry should recognize that most users will be unfamiliar with the technical details. Industry needs to explain these processes simply based on what the user needs to achieve.

2. Use Case #2 – Health Information Exchange

The Cures Gateway Architecture workstream used is illustrated in Figure 8. Invitae led this effort using the Ciitizen platform as the test patient health application (PHA). While this approach was the only approach we tested that was proprietary, we believe it offers the only known way in which an individual can federate their digital identities with HIEs to access their own health information via the IHE protocols.

Figure 8. Cures Gateway Architecture



Testing Process and Final Report Out	
Description of User Journey	
Steps necessary for a PHA and an HIE to trust one another and enable data exchange through a secure intermediary gateway (Invitae)	• Invitae and HIEs establish contractual relationships: ○ Invitae, already a HIPAA-covered entity, becomes a business associate of HIEs (although the Gateway serves only as a conduit of PHI from HIEs to PHAs, the parties enter into a business associate agreement to resolve any uncertainties).

	○ Invitae and HIEs agree on exchange protocols (IHE or HL7® FHIR®). ○ HIEs and Invitae agree to a set of contractual terms common to HIE participant agreements. The purpose of the exchange is solely to enable patients to obtain their health information from a participating HIE, whether through a PHA or patients acting on their own. • Invitae and PHAs establish contractual relationships. • PHAs apply for access and are vetted by Invitae as follows: ○ PHAs attest to the CARIN Code of Conduct or similar. ○ PHAs must identity proof their users to IAL2 via a Kantara-certified identity provider (IdP) vendor. ○ PHAs must demonstrate that they are acting on behalf of the patient to obtain data for the patient's use. ○ PHAs must demonstrate that they obtain the consent of the patient to search for the health information from all places where they have obtained care. ○ PHAs complete the security questionnaire from the CARIN Code of Conduct; answers are shared with patients on a Gateway webpage. ○ The Ciitizen PHA is held to the same standards as other PHAs connected to the Gateway. • Invitae and PHAs agree on exchange protocols (HL7® FHIR®). • Configuration steps require manual configuration between the Gateway and each HIE, and between the Gateway and each PHA. • HIEs can review PHA application materials and may reject any Invitae-approved PHA from being able to query their data (HIE may be subject to an info-blocking challenge by the PHA if it is an unwarranted block). • Queries are limited to patients ages 18 and older.
The user journey steps	• User chooses to access data through a PHA (users without a PHA onboard for identity proofing and payload delivery purposes through a temporary Ciitizen PHA account). • User conducts a one-time identity proofing event at NIST 800-63-3 IAL2 that the PHA supplies. • User consents to enabling a records search using identity attributes information taken from the IAL2 process. • PHA passes authenticated demographics to Invitae Cures Gateway over a secure channel.
Pass-through of ID-proofed demographics from Invitae Cures Gateway to HIEs	• Having accepted a valid and consented records request from PHA, Invitae Cures Gateway queries all available HIEs for the patient as follows:

	○ Validated demographics are presented to each HIE for a patient lookup using the agreed protocol (e.g., IHE, HL7® FHIR®, custom). ○ HIEs use a demographic search to determine if a single patient in their database uniquely matches the patient. ○ If zero matches, or two or more matches are found, an appropriate denial message is returned to the gateway. ○ If exactly one match is found, a "patient found" message is returned to the gateway. • For "patient found" messages, the gateway responds with a record request for all documents for the patient. ○ Most return an on-demand created Clinical Document Architecture (CDA) or C32 XML document. ○ Some also return additional documents or data not contained in the generated XML. ○ For patients temporarily onboarded to the Ciitizen PHA for purposes of ID proofing and payload delivery, those patients have up to 30 days to download their data. • The Invitae Cures Gateway temporarily stores the returned documents from the responding HIEs as HL7® FHIR® resources. • The Invitae Cures Gateway notifies the requesting PHA whether documents have been found. PHA either alerts the patient that no records were retrieved or collects the stored records from the Invitae Cures Gateway. • The Invitae Cures Gateway deletes patient documents once delivered to the PHA.
Participants in the Use Case	
1. Credential Service Providers: ID.me and Persona 2. Health Information Exchanges: HIEs connected to the Cures Gateway 3. Personal Health Applications: Ciitizen and OtisHealth 4. Observers: Kantara Initiative	
Description of How the Use Case Was Tested	
Pre-production testing	• Participating HIEs store a common test patient in their Master Person Index (MPI) and data lake. • Invitae disables identity proofing to query a test patient. • The patient is found, and data is returned. • Data is compared and validated in PHA.
Production testing	• The user, a consented HIE staff member with data stored in HIE, signs onto PHA. • The user goes through the identity proofing process. • The user consents and requests records. • The user views returned record(s) in PHA.

	• The process is repeated with another HIE staff member or family member. The workgroup recorded a video demo of the process, which can be viewed on the CARIN Alliance YouTube page.
Lessons Learned	

Benefits	• Users can use one trusted credential to interact with multiple HIEs, which in turn represents data from multiple healthcare systems, physician practices, diagnostic labs, radiology centers, etc.
	• Patients/users can get their full medical record downloaded into their PHA using a single query to all participating HIEs without needing to:
	  ○ Remember portal credentials.
	  ○ Remember all sites and health systems where they may have data.
	• HIEs and the participating covered entities within their service area can meet the 21st Century Cures Act with a single connection to the Invitae Cures Gateway.
	• Patients have a growing list of PHAs to use.
	• Patients can use self-service to request and obtain their medical records.

How the industry can improve	• At present, Invitae uses contractual agreements between the Gateway and the HIEs to ensure the gateway will only query HIEs for consented, identity-proofed patients.
	  ○ Any review requires looking through the audit logs to verify conformity.
	  ○ Improvements to protocols can be made so that consent certificates and IdP certificates can be passed, which would add to trust levels and avoid the need for most reviews, if those consent and IdP certificates persist across queries over time versus burdening the patient by requiring those processes to be initiated with every query.
	• Invitae uses contractual agreements between the Gateway and PHAs to ensure the PHA will only query through the Gateway with consented, identity-proofed patients.
	  ○ As above, improvements to protocols to carry certificates of consent and IdP could add trust levels up the chain if done in a way that does not add burden to the patient.

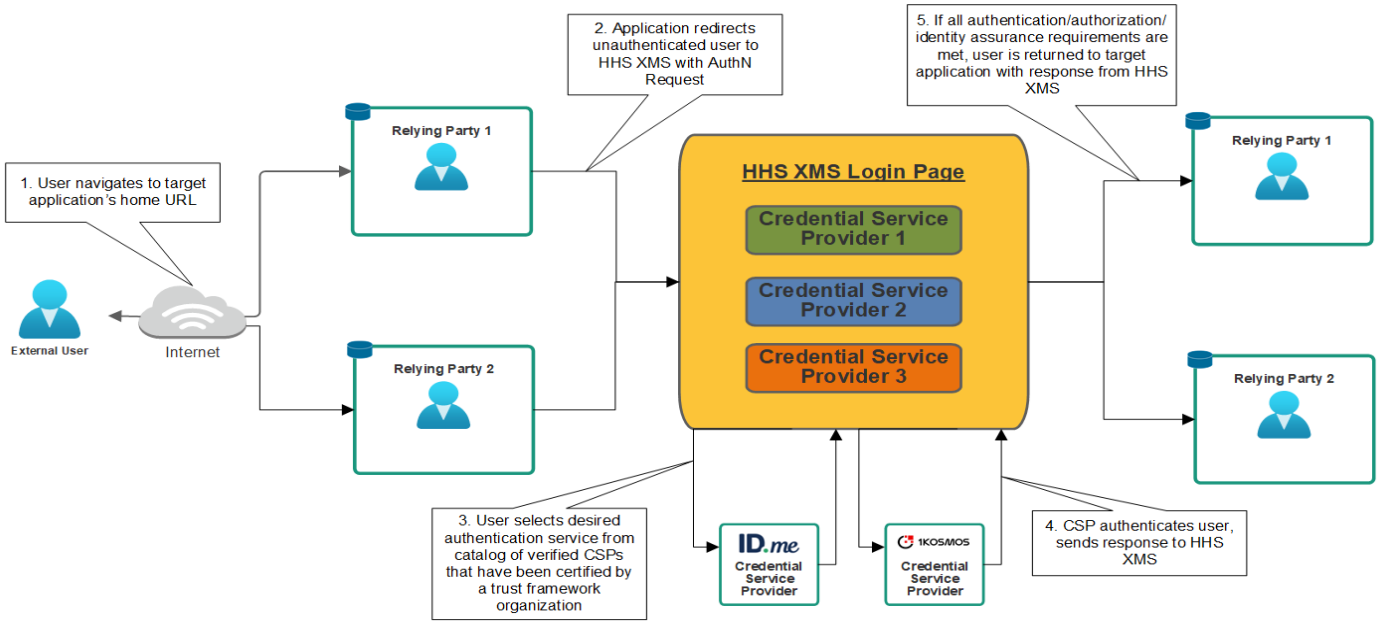
3. Use Case #3 – HHS NextGen External User Management System (XMS)

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

How HHS XMS works:

- Upon successful integration, users wanting to access the relying party application will be routed to HHS XMS for authentication and identity proofing processes.
- Within HHS XMS, users will be presented with a list of CSPs from which to choose.
- If the user is required to complete identity proofing (IAL2), HHS XMS will include this information in the authentication request to the CSP.
- After successful authentication, HHS XMS will share the user information with the relying application party to initiate the application session. See Figure 9 for details.

Figure 9. HHS XMS Use Case Flow



The HHS XMS workgroup applied the following assumptions to the workstream.

Credential Service Provider

- HHS XMS will leverage ID.me and 1Kosmos as CSPs for creating, maintaining, and managing PoC user accounts.
- PoC users will create their CSP credentials via the CSP account creation page. The CSP will provide guidance on account creation.
- The CSP Helpdesk will provide support for issues related to CSP credentials.
- The CSP team will participate and provide necessary support to integrate the credentialing processes with HHS XMS.

Applications

- Interested applications for the PoC will support OIDC or Security Assertion Markup Language (SAML) federated protocols and web-based applications; these are requirements for integration.

- Integrated applications for the PoC will require IAL2.
- Identity proofing of individuals requesting to affiliate with an organization as a member will be the responsibility of the organization's administrator. This identity proofing process will be conducted outside of HHS XMS as a delegated identity proofing process.

General

- An external ID (XID) will be generated in HHS XMS for each PoC user account to correlate attributes between HHS XMS and the integrated applications.
- HHS will participate in finalizing the PoC user acceptance test (UAT) cases and will make UAT testers available for execution and acceptance.
- The desktop and mobile HHS XMS solution is supported on a subset of browsers.

Testing Process and Final Report Out	
Description of User Journey: User Registration – ID.me (TC001)	
User journey steps: Verify that users can create ID.me Credentials	• Pre-requisites: The test must be performed using the HHS XMS desktop site, the user does not have existing ID.me credentials, the user does not have an active email account/address that can be accessed, and the user does not have any active sessions. • Navigate to HHS XMS login page and select the "Sign in with ID.me" button from the HHS XMS dashboard of sign-in options. • After redirection to the ID.me sign-in page from HHS XMS, create an ID.me account by entering in a valid email address and password and accepting ID.me Terms of Service and Privacy Policy. • Complete email verification process and enroll in mandated multi-factor authentication (MFA) to close out test case (TC) 001.
Participants in the Use Case	
1. Credential Service Provider: ID.me 2. Identity Broker: HHS XMS 3. Relying Parties: Marshfield Clinic and Patient Centric Solutions	
Description of How the Use Case Was Tested	
• Test scenarios and the correlated steps, developed by the identity broker team (HHS XMS), were distributed to the identified RP testers (Patient Centric Solutions and Marshfield Clinic). Testers were advised to execute their assigned test scripts offline and at their convenience. Each test scenario was outlined in a workbook documenting the user action needed, user input/data elements required, and expected output for the user to self-identify whether they have successfully completed each test scenario step. The identity broker team (HHS XMS) conducted several live working sessions to walk testers through the outlined test scenario steps and troubleshoot where needed.	

Test Data Used
• Test User Identities: N/A   ○ Testers created personal accounts to walk through this test scenario given that CSP accounts (ID.me and 1Kosmos) were previously created under test user email accounts.

Testing Process and Final Report Out	
Description of User Journey: User Identity Proofing – ID.me (TC002)	
User journey steps: Verify that users can verify their identity with ID.me to IAL2/AAL2	• Pre-requisites: The test must be performed using the HHS XMS desktop site, the user has an active session from execution of TC001, the user has an active HHS XMS account with ID.me credentials, the user has not identity proofed previously, and the user has a device with camera capability. • In the active ID.me session, upload a photo of your license, state ID, passport, or passport card to begin the identity proofing process. • To complete the unsupervised-remote flow, take and submit a video selfie. Note: In the supervised-remote flow, a user may speak with a trusted referee (video-chat agent). In this flow, a user may verify at IAL2 without using biometrics. Additional pieces of identity evidence may be leveraged as well here. • Enter a synthetic Social Security Number when prompted by ID.me flows. Note: User to enter a synthetic Social Security Number, NOT their real Social Security Number, as this is a test environment. • Test case (TC) 002 is complete and end user has successfully identity proofed with ID.me. An HHS XMS account is created and verified at IAL2.
Participants in the Use Case	
1. Credential Service Provider: ID.me 2. Identity Broker: HHS XMS 3. Relying Parties: Marshfield Clinic and Patient Centric Solutions	
Description of How the Use Case Was Tested	
• Test scenarios and the correlated steps, developed by the identity broker team (HHS XMS), were distributed to the identified RP testers (Patient Centric Solutions and Marshfield Clinic). Testers were advised to execute their assigned test scripts offline and at their convenience. Each test scenario was outlined in a workbook documenting the user action needed, user input/data elements required, and expected output for the user to self-identify whether they have	

successfully completed each test scenario step. The identity broker team (HHS XMS) conducted several live working sessions to walk testers through the outlined test scenario steps and troubleshoot where needed.
Test Data Used
• Test User Identities: N/A   ○ Testers created personal accounts to walk through this test scenario given that CSP accounts (ID.me and 1Kosmos) were previously created under test user email accounts.

Testing Process and Final Report Out	
Description of User Journey: Positive Patient Matching – ID.me (TC003)	
User journey steps: Verify that HHS XMS directs PatientShare application users to the PatientShare application after successful authentication to HHS XMS (via ID.me credentials) when PatientShare application URL is accessed directly (via bookmark or typing in the PatientShare application URL) on a desktop	• Pre-requisites: The test must be performed using the HHS XMS desktop site, the user has an active HHS XMS account (using ID.me credentials) at IAL2, the user has an active account in the relying party application, and the user does not have any active sessions. • Navigate to HHS XMS login page and select the "Sign in with ID.me" button from the HHS XMS dashboard of sign-in options. • After redirection to the ID.me sign-in page from HHS XMS, log into ID.me with test credentials (IAL2/AAL2 for the Betsy Smith persona). • Upon successful login, the user is directed to the relying party application homepage via HHS XMS authentication.
Participants in the Use Case	
1. Credential Service Provider: ID.me 2. Identity Broker: HHS XMS 3. Relying Parties: Marshfield Clinic and Patient Centric Solutions	
Description of How the Use Case Was Tested	
• Test scenarios and the correlated steps, developed by the identity broker team (HHS XMS), were distributed to the identified RP testers (Patient Centric Solutions and Marshfield Clinic). Testers were advised to execute their assigned test scripts offline and at their convenience. Each test scenario was outlined in a workbook documenting the user action needed, user input/data elements required, and expected output for the user to self-identify whether they have successfully completed each test scenario step. The identity broker team (HHS XMS) conducted	

several live working sessions to walk testers through the outlined test scenario steps and troubleshoot where needed.
Test Data Used
• Test User Identities: Betsy Smith

Testing Process and Final Report Out	
Description of User Journey: User Registration – 1Kosmos (TC004)	
User journey steps: Verify that users can create 1Kosmos Credentials	• Pre-requisites: The test must be performed using the HHS XMS desktop site, the user does not have existing 1Kosmos credentials, the user does not have an active email account/address that can be accessed, and the user does not have any active sessions. • Navigate to HHS XMS login page and select the "1Kosmos" button from the HHS XMS dashboard of sign-in options. • After redirection to the 1Kosmos sign-in page from HHS XMS, create a 1Kosmos account by entering in a valid email address and verifying that email address. The user will complete a registration form including First Name, Last Name, a valid phone number, and password, and be required to verify phone number. • Test case (TC) 004 is complete and end user has successfully created an account with 1Kosmos; HHS XMS account created at IAL1.
Participants in the Use Case	
1. Credential Service Provider: 1Kosmos 2. Identity Broker: HHS XMS 3. Relying Parties: Marshfield Clinic and Patient Centric Solutions	
Description of How the Use Case Was Tested	
• Test scenarios and the correlated steps, developed by the identity broker team (HHS XMS), were distributed to the identified RP testers (Patient Centric Solutions and Marshfield Clinic). Testers were advised to execute their assigned test scripts offline and at their convenience. Each test scenario was outlined in a workbook documenting the user action needed, user input/data elements required, and expected output for the user to self-identify whether they have successfully completed each test scenario step. The identity broker team (HHS XMS) conducted several live working sessions to walk testers through the outlined test scenario steps and troubleshoot where needed.	

Test Data Used
• Test User Identities: N/A   ○ Testers created personal accounts to walk through this test scenario given that CSP (ID.me and 1Kosmos) accounts were previously created under test user email accounts.

Testing Process and Final Report Out	
Description of User Journey: Positive Patient Matching – 1Kosmos (TC005)	
User journey steps: Verify that HHS XMS directs PatientShare application users to the PatientShare application after successful authentication to HHS XMS (via 1Kosmos Credentials) when PatientShare application URL is accessed directly (via bookmark or by typing in the PatientShare application URL) on a desktop	• Pre-requisites: The test must be performed using the HHS XMS desktop site, the user has an active HHS XMS account (using 1Kosmos credentials) at IAL2, the user has an active account in the relying party application, the user does not have any active sessions, the user has an active email address and/or SMS-capable phone number that can be accessed, and the user has notified HHS XMS of 1Kosmos created account (see TC004) so HHS XMS can set the IAL level of the HHS XMS account to IAL2 per relying party application requirements. • Navigate to the relying party URL on desktop and be redirected to HHS XMS login page. • On the HHS XMS login page, select the “1Kosmos” button from the HHS XMS dashboard of sign-in options. • Enter 1Kosmos username, password, and one time passcode (OTP). • Upon successful authentication, the user is directed to the relying party application homepage.
Participants in the Use Case	
1. Credential Service Provider: 1Kosmos 2. Identity Broker: HHS XMS 3. Relying Parties: Marshfield Clinic and Patient Centric Solutions Additional workgroup observers included b.well, DirectTrust, Kaiser Permanente, MaxMD, and Security Health Plan	
Description of How the Use Case Was Tested	
Test scenarios and the correlated steps, developed by the identity broker team (HHS XMS), were distributed to the identified RP testers (Patient Centric Solutions and Marshfield Clinic). Testers were advised to execute their assigned test scripts offline and at their convenience. Each test scenario was outlined in a workbook documenting the user action needed, user input/data elements required, and	

expected output for the user to self-identify whether they have successfully completed each test scenario step. The identity broker team (HHS XMS) conducted several live working sessions to walk testers through the outlined test scenario steps and troubleshoot where needed. The workgroup recorded a video demo, which can be viewed on the CARIN Alliance YouTube page.
Test Data Used
• Test User Identities: Betsy Smith

Lessons Learned	
What worked	• The PoC between HHS XMS as the identity broker and two RPs successfully supported integrations over multiple protocols (e.g., SAML 2.0 and OIDC). Optionality to end users was proven through the ability of testers to self-select their preferred credential service provider (CSP), such as ID.me or 1Kosmos, in addition to portability where existing user accounts (via test data) were leveraged to reduce friction in the user experience enabling the same user to access relying parties using different HHS XMS-integrated authentication providers. HHS XMS integrations with multiple CSPs quicken the user onboarding process for the transient/external user population. Furthermore, the HHS XMS abstraction layer manages these CSP integrations and implements changes in line with federal mandates (e.g., NIST standards) and emerging needs, minimizing the disruption to the user experience and the relying parties. Moreover, the PoC integrations further proved that a user could bring their own identity from a verified CSP and access relying party applications without having a direct integration between a CSP and RP. The UAT results were as follows: ○ Criteria #1: RP identified testers completed seven required test scripts. ▪ Result: All (100%) of the test cases planned for the final testing cycle were executed. ○ Criteria #2: If any test script has a "fail" status and has not been resolved before testing ends, appropriate resolution steps must be documented. ▪ Result: All (100%) of the test cases planned for UAT passed. No test cases had a "fail" status.
What did not work and why	• The identity verification process flow for test users and test data for blockchain-based CSPs introduced friction to the user experience. Blockchain-based CSPs tested in this PoC were unable to identity proof fictional personas using test user attributes and sample identity documents because of underlying controls imposed by the blockchain technology. Development of testing procedures and environments considering test data and validation

	will create a better development and integration experience between blockchain-based CSPs and identity brokers.
How the industry can improve	• Consistent identity authentication and patient matching attribute naming conventions and formats across the industry would enhance the interoperability of integrations between industry players. For example, the HHS XMS team noted two defects caused by identity attribute improper formatting during the testing cycle and have documented them in the table below. ○ Note: ID.me can support OIDC standards for naming conventions with a small update to the property names on a per-policy basis. • HHS XMS and the federated CSPs each have a unique ID for a given user. There are workflow benefits when CSPs (authenticators) deliver a unique user ID along with their other claims, particularly for patient matching as these unique IDs get stored with multiple RPs. If a user chooses to use the same CSP for the CSP flow and the HHS XMS flow, each would return a different unique ID. Given that users have the same choice, one would expect them to select the same CSP. Though the HHS XMS flow returns the same ID independent of the CSP chosen (a unique benefit), it would also be beneficial in use cases where RPs have a relationship with a particular CSP to have access to the unique identifiers from that CSP. It would be helpful to identify standards and processes to capitalize on unique user IDs coming from authenticators and establish a mechanism for HHS XMS to provide both its unique external ID (XID) and the unique ID of the CSP account used to authenticate by the user. • By design, HHS XMS self-service integration capabilities are available only to HHS employees and contractors who are tasked with owning or managing HHS-owned applications. This restriction resulted in a lack of access to technical implementation documentation to non-government entities and introduced additional steps required for offline coordination of the configuration. If commercial entities are to leverage the same HHS XMS instance for healthcare, a process will need to be defined to provide equivalent access capabilities for commercial entities that match those provided to government entities integrating with HHS XMS.

Figure 10. HHS XMS Identified Defects Summary

Defect ID	Status	Priority	Type	Description	Identified By	Test Scripts	Date Identified	Assigned To	Defect Resolution
UAT-001	Closed	Low	Defect	In ID.me positive patient matching scenario, the end user was directed to the relying party application upon logging in with ID.me user persona (Betsy Smith) credentials. However, the payload with additional identity attributes (e.g., address, DOB, etc.) was improperly formatted and the relying party application was unable to read as a result.	Relying Party - Identified Tester	TC003	12/19/2022	Identity Broker - HHS XMS Technical Representation	HHS XMS updated the formatting of the payload and pushed a fix so that the end user is directed to the relying party application. Relying party team retested the fix and confirmed the defect has been resolved. Note: ID.me can support OIDC standards for naming conventions with a small update to the property names on a per-policy basis.
UAT-002	Closed	Low	Defect	In 1Kosmos positive patient matching scenario, the end user was directed to the relying party application upon logging in with ID.me user persona (Betsy Smith) credentials. However, the payload with additional identity attributes (e.g., address, DOB, etc.) was improperly formatted and the relying party application was unable to read as a result.	Relying Party - Identified Tester	TC005	12/19/2022	Identity Broker - HHS XMS Technical Representation	HHS XMS updated the formatting of the payload and pushed a fix so that the end user is directed to the relying party application. Relying party team retested the fix and confirmed the defect has been resolved.

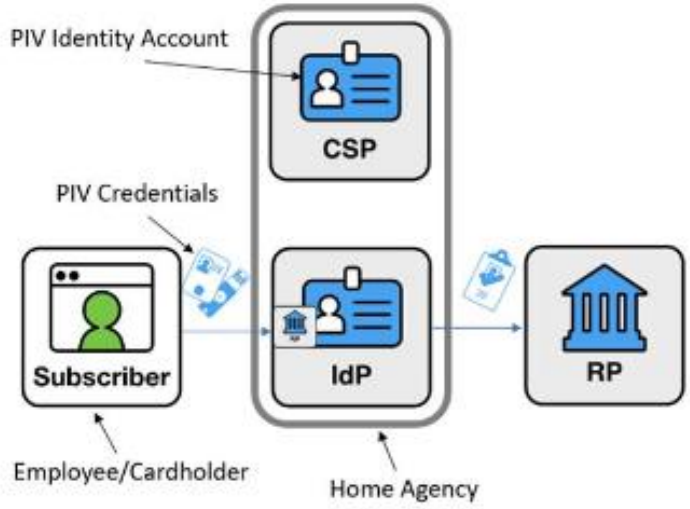
HHS XMS Federal Assurance Level (FAL) Workflow

HHS XMS would like to conduct future testing in compliance with NIST 800-63-3 FAL requirements. The HHS XMS solution is able to:

- Provide a recommended way to accept and process personal identity verification (PIV) credentials from other agencies.
- Provide real-time sharing and identity assertions and attributes from the PIV account at cardholder's home agency.
- Facilitate interoperability between applications and a variety of authenticators.
- Allow use of non-PKI-based derived PIV credentials across domain boundaries.

In these cases, the IdP must be associates with the issuing agency. The subscriber will log into the IdP with their derived credential and federation protocol will then allow the subscriber to log into the RP.

Figure 11. HHS XMS Personal Identity Verification Flow



4. Use Case #4 – CSP with UDAP™ Tiered OAuth

This workgroup leveraged the HL7® UDAP™ Tiered OAuth Security standard. Tiered OAuth steps include:

1. The user authorizes a client application (e.g., PHA).
2. The user authenticates with a federated CSP.[6]
3. The data holder/relying party obtains a token directly from the CSP.
4. The data holder/relying party releases data via HL7® FHIR® to the user's Client Application. This outcome reflects trust validation and any local policy.

This workflow is nearly identical to conventional SMART on FHIR®, except instead of needing credentials issued by every data holder, the matching, with verified demographic attributes or the CSP-assigned digital identifier (before the responder links the identity to a local patient identifier), uses data from a trusted third-party CSP. Demographics are passed securely from the CSP directly to the relying party data holder as a client of that CSP (see red arrows in Figure 11). This workflow gives the individual user the ability to authenticate using any CSP and access data from any relying party that has implemented Tiered OAuth, providing flexibility and choice to the end user who only needs to get ID proofed by one CSP to pull data from any compatible data holder.

In this scenario, there is no point-to-point integration or manual configuration. Instead, a trust framework enables dynamic discovery and trust of other parties in the transaction, enabling automation and therefore scalability of ecosystem participants via publicly available standards. As an additional benefit, digital certificates may be used to secure consumer-facing client applications and are recommended when data holders take on the role of client to a third-party identity service they are relying on. The UDAP™ framework is included in the HL7® FHIR® Roadmap for TEFCA Exchange, TEFCA Facilitated HL7® FHIR® Implementation Guide, Carequality HL7® FHIR® Exchange Implementation Guide, HL7® Security recommendations, and the ONC's Interoperability Standards Advisory.

[6] The data holder/relying party successfully validates trust with the CSP via a Trust Anchor and vice-versa, just as a Client Application may validate trust with the data holder and vice-versa, per UDAP™.

Figure 12. UDAP™ Tiered OAuth

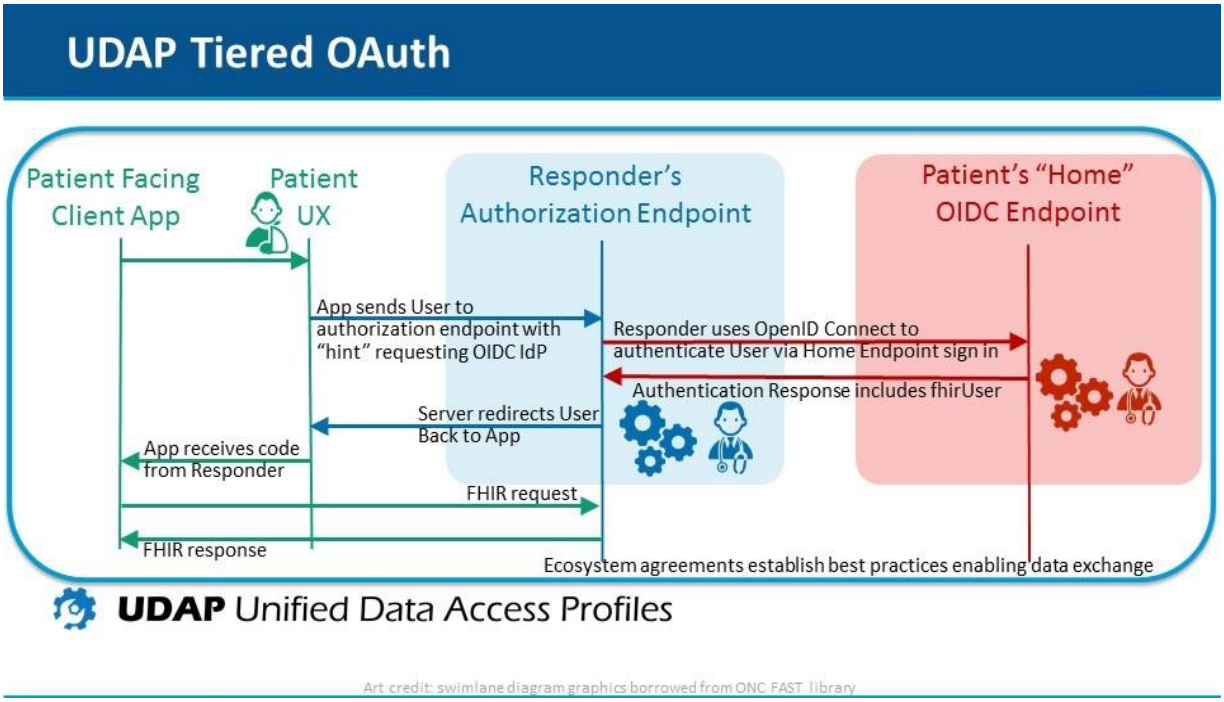


Figure 13. UDAP™ Tiered OAuth For User Authentication Detailed Flow

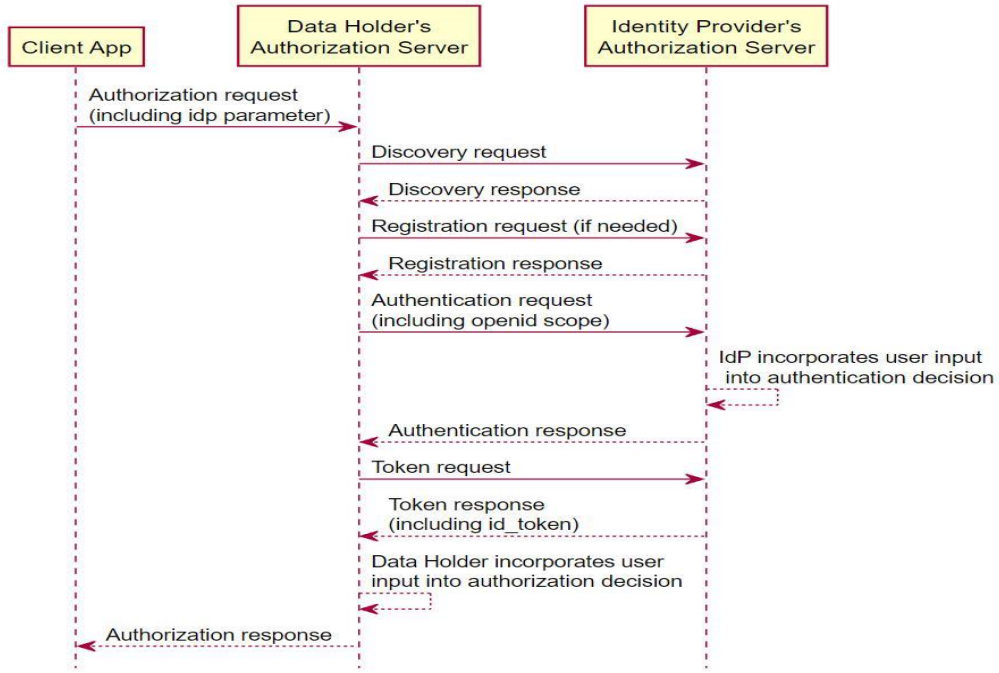


Image Source: HL7®/UDAP.org™ Security for Scalable Registration, Authentication and Authorization. Please refer to the Implementation Guide for more information regarding UDAP™ Tiered OAuth and the diagram above.

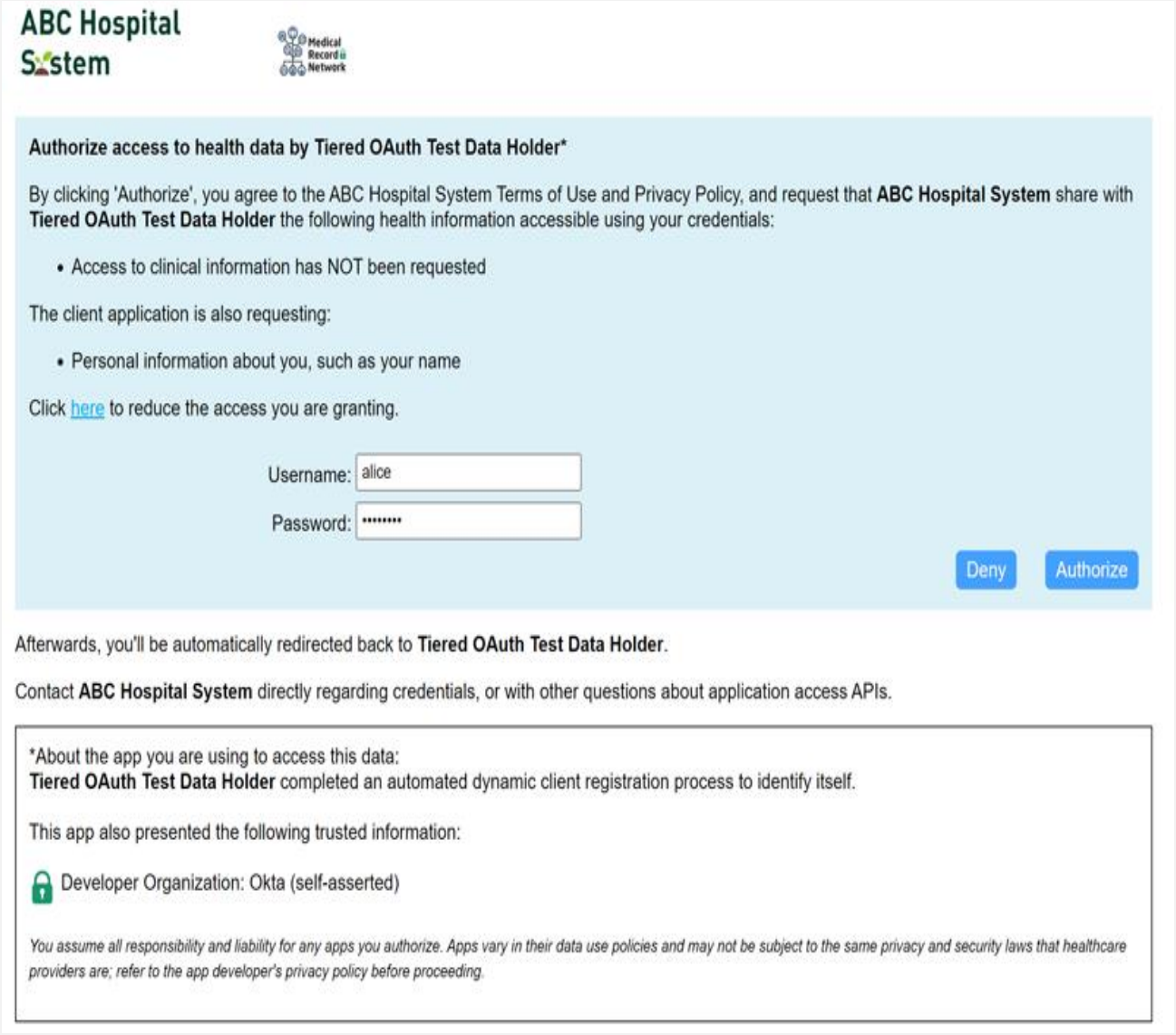
The workgroup determined its use cases by reviewing the background from the HL7® connectathon track (FAST Infrastructure Scenario #4), which this PoC workstream mirrors. The workgroup decided to assess:

- UDAP™ Business to Consumer (B2C) with Tiered OAuth
- UDAP™ Business to Business (B2B) with Authorization Extension Object

Testing Process and Final Report Out	
Description of User Journey	
Description	• This use case is designed for interactions that dynamically validate trust between all parties. • Participants implement UDAP™ workflows (extensions of OIDC & OAuth) and the client, relying party data holder, and CSP validate trust without any prior one-off interaction. • Participants agree on ecosystem-wide assurance levels (IAL and AAL) and identity attributes to share as claims. • Client, CSP, and RP obtain certificates from a trusted certificate authority and are thereby also trusted by others in the ecosystem. • This use case has a publicly discoverable authorization endpoint, token endpoint, and identity service endpoint.
User journey steps	• User initiates a query to the data holder's system through a certificate authority and selects a CSP to authenticate themselves. • Data holder validates trust with the CSP and registers with the CSP dynamically if a previous relationship does not yet exist. The data holder redirects the user to the CSP to sign in. • The user completes identity verification and creates a credential with the CSP if it does not already exist. • The user consents to share requested identity attributes with the data holder. • The user is redirected to the data holder and authorizes the release of health data from the data holder to the client application. If the data holder can match on the patient with sufficient confidence, the data holder sends data to the client.
Participants in the Use Case	
• Credential Service Providers: Evernorth, EMR Direct, and Okta • Relying Parties (Data Holders): Evernorth, EMR Direct, and Okta • Observers: 1Kosmos, b.well, Cedars-Sinai Medical Center, and OtisHealth Additional participants have previously and again recently tested UDAP™ B2B and B2C flows at HL7®, Carequality, CommonWell and CMS HL7® connectathons) and a few implementers are collaborating to build open source reference implementations to complement the publicly available standards. A testing tool and community support discussion group is available for the UDAP™ framework.	

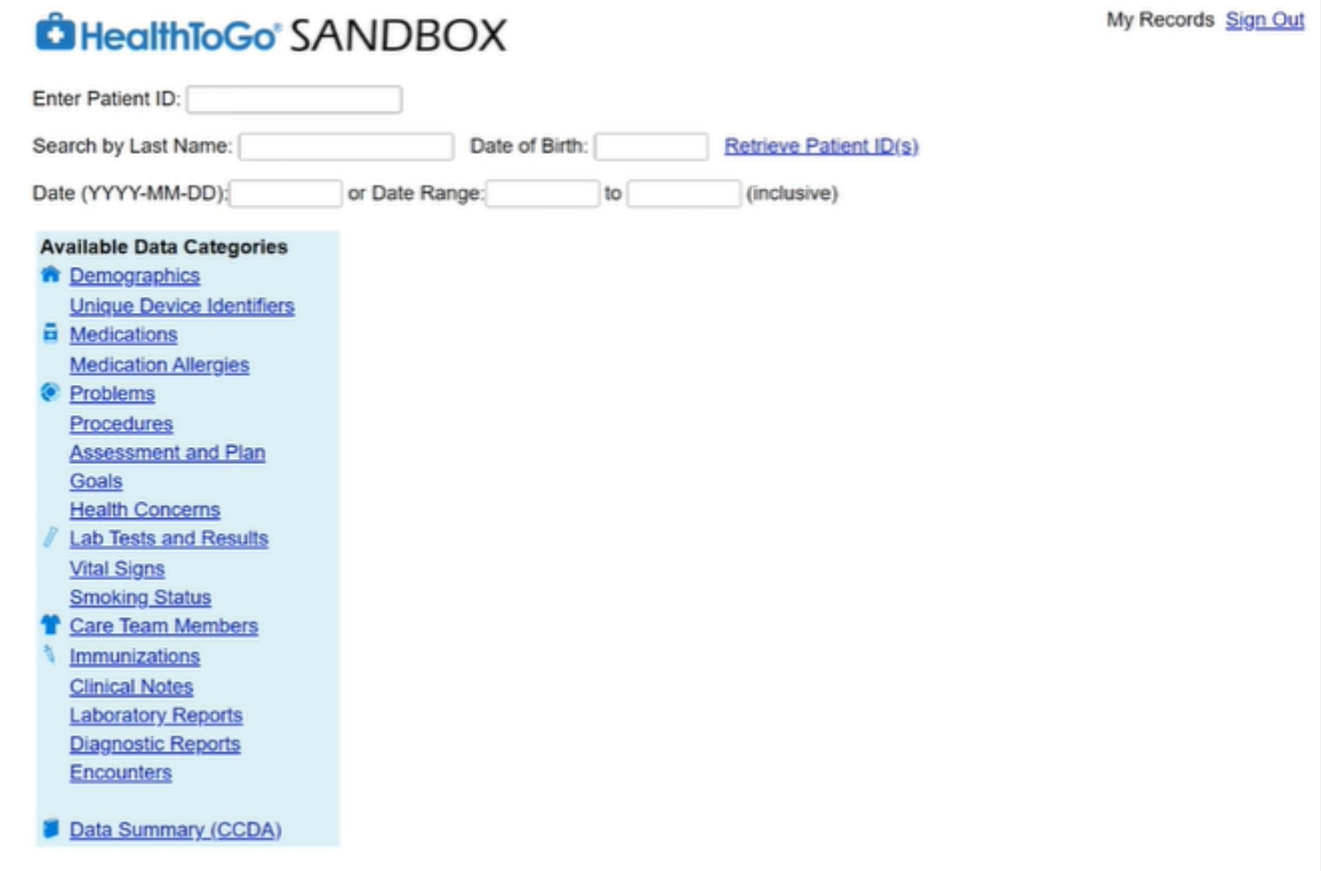
How the Use Case Was Tested

- Client (EMR Direct HealthToGo) invokes UDAP™ Tiered OAuth and the patient end user is directed from the Data Holder's OAuth sign in page (where the patient's authorization of data transfer to client is captured) to the sign in page at the third-party CSP (EMR Direct/ABC Hospital System). At that point, the data holder (Okta/Tiered OAuth Test Data Holder) takes on the role of client to that CSP in a conventional OIDC/OAuth workflow, and the patient authenticates to the trusted CSP using the form below.



- Note that the client only navigates the user to this page after verifying that the CSP is trusted by validating its digital certificate. This process includes confirmation that the certificate chains up to an acceptable trust anchor, so the user can be confident about where they are entering their credentials. Within the page, the UDAP™ Green Lock displayed by the CSP indicates that the data holder is also using a trusted digital certificate, so the user can feel confident about where personally identifiable information is allowed to be shared.

- After successful authentication with the third-party CSP, patients view their health data from the data holder's system within the client application.



- The workgroup recorded a video demo, which can be viewed on the CARIN Alliance YouTube page.

Test Data Used
• The workgroup anticipates leveraging common test users in future testing sessions to refine the test scenario.

Lessons Learned	
Benefits	• No advance testing or integration is required by ecosystem participants (client application, RP data holder, and credential service provider implement UDAP™ profiles and use real-time discovery and trust validation) for true scalability. • Patients can use one trusted set of credentials representing their identity to interact with multiple healthcare systems, meaning fewer credentials need to be maintained. • Health record systems have high confidence about which patients have been authenticated, as well as protection from

	breach severity knowing they are using publicly available security and patient matching standards, particularly if the hl7_identifier is used for more perfect patient matching. • CSPs complying with the Identity IG will also share an interoperable digital identifier that is unique to the patient and can be used for high-confidence patient matching. Whether the patient uses just one CSP at every point of care or a few different ones, this identifier can be used to create a complete history of each patient's records. • Even though this workstream is the most technically complex conceptually, the integration is designed to be lightweight for those already implementing Cures, and the scalability benefit is, therefore, potentially the highest.
What did not work and why	• Some manual intervention was required to do patient matching. The UDAP™ Tiered OAuth team will more formally use publicly available test users to better demonstrate digital identity reusability at future events (such as ONC Health IT certification program test patients).
How the industry can improve	• Communicate the industry benefit of more consumer choice in high assurance digital identity based on standards. • Communicate the security benefits of using common standards, setting an IAL2/AAL2 floor. • Emphasize the affordability of reusable identity services. • Ultimately, having a directory of CSPs will automate CSP discovery. • UDAP™ Dynamic Registration & UDAP™ JWT-Based Authentication provide scalability benefits and were used exclusively by participants in PoC testing. Without these, manual registration will be less scalable and client confidentiality less secure.

Conclusions

Participants benefited from the opportunity to convene and discuss how to collaborate to improve consumer-directed exchange. Additional testing and collaboration among and across the various workstreams will be beneficial by continuing to apply the end user experience gained toward the various solution options. For example, one workstream's participants shared examples with all groups of attributes, namely SSN Last 4, that can be highly useful to their system in matching across organizational boundaries. Another workstream participant provided a consumer research example of individuals expressing comfort in the use of this attribute in person matching, while striking a privacy preserving balance. The PoC also led to a conversation about the period of interest for a search and the value of the previous address attribute in patient matching. This feeds back into standards development initiatives for further consideration. Additionally, the need for a standardized individual identifier expressed in the HHS

XMS use case workstream is addressed by the Digital Identifier within the HL7® Identity standard that the CSP with UDAP™ workstream uses. This methodology is likely to be a topic of community conversation during future testing as these identifiers begin to percolate into transactions because their use allows systems to forego probabilistic matching entirely.

Preferred 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 a 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.

Both options will enable the healthcare ecosystem to allow individuals the ability to identity proof themselves once, establish their own digital identity credential, and then use that digital credential across multiple relaying parities as their own 'single sign on' for U.S. healthcare. We do not believe we need to recommend one of these options over the other. In fact, we believe both options could work well together given there has been preliminary interest in HHS XMS adopting the UDAP™ Tiered OAuth protocol. We look forward to future digital identity federation pilots where these two protocols can be tested across multiple relying parties. We invite others who are interested in testing these approaches to contact the CARIN Alliance via our website.

Recommendations and Lessons Learned for Future Testing

Patient Factors

- Involve more patient users and other constituents (including caregiver proxy representation) to evaluate 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 when patient privacy and individually identifiable data and health data are considerations.
- Employ fictional test users and test data at the beginning of the experiment based on the ONC EHR Test Data.
- Convey feedback to FAST Security and Identity to refine the OIDC assertion profile documented in Section 5.2 of the Identity Implementation Guide, which extends OpenID Connect Core Standard Claims from Section 5.1.

- Convey any new feedback to FAST Identity 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 SSN Last 4, mobile phone numbers, email addresses, and other attributes.
- Encourage CSPs to establish processes for collecting and validating attributes essential to identity resolution at relying party systems during ID proofing.
- Include processes and profiles for CSPs to include historic addresses within the assertions sent to data holders because data holders may have stale information about a patient's previous address and may fail to match if the CSP only asserts the most recent patient address.

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 two RP participants to adequately test the interoperation between all parties at scale in a dynamic or automated fashion.
- 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 and should be evaluated. We are currently examining financial models that are working outside the US and will be evaluating them as part of a subsequent testing event.

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.

Areas for Future Engagement

General Testing Considerations

- Test the UDAP™ B2B with Authorization Extension Object.

- Address IAL2 gaps for certain users, such as minors (please see the Appendix for more information on minor identity).
- Test passing tokens or certificates along with the query in the HIE testing environment to bolster trust associated with contractual commitments.
- Ensure compliance with the NIST Federation Assurance Level (FAL) requirements.

Further Testing of the UDAP™ Tiered OAuth Functionality

- PoC participants will conduct further UDAP™ Tiered OAuth testing in the coming months. Participants intend to test UDAP™ Tiered OAuth functionality more wholistically across additional participants in various roles.
- PoC participants can partner with the FAST Identity Team on future HL7® connectathon tracks for the UDAP™ Tiered OAuth testing.

User Experience

- Explore the user experience in XMS (and other workstreams) — from registering with an individual CSP to building out an XMS account to supporting multiple forms of credentials and accessing multiple different CSPs — to understand the best way to introduce the brokered system to end users and walk them through establishing multiple credentials for the same profile.
- Consider the impact on patients (and entities offering individual access services) of any model that requires patients to go through IdP and consent flows for each query.

Attribute Format Standardization

- Focus on standardizing the formats of shared attributes to help accelerate the integration process, as well as fleshing out how those attributes are handled after the first time they are passed through to the RPs (for example, discussing the expectations from RPs for verifying attributes and how they should be handled if they change from the upstream source or if there is a conflict from other patients).

Privacy and Transparency

- Address privacy concerns for data collection and use during the identity proofing process.
- Develop a collective understanding of how identity attributes are handled, what information is logged, and why it is necessary to do so, and provide end users with the opportunity to acknowledge that they comprehend these standards.
- Develop a privacy policy that addresses whether data is aggregated for email addresses and/or on identity use of that data.

Minor Identity

- Develop workflows identifying an open framework for identity proofing minors with their consent and their legal guardian/parental consent. The CARIN Alliance has started a minor's identity workgroup to begin working on this topic. Please see the appendix for our initial thinking on minor's identity.

Improve Awareness and Adoption

- Promote adoption of this work in the patient and provider communities as it moves toward pilot and production stages.

Appendices

Appendix A. Master Participant List

ROLE	ORGANIZATION
APPLICATION	❖ b.well ❖ Invitae ❖ MaxMD ❖ OtisHealth ❖ Patient Centric Solutions
CREDENTIAL SERVICE PROVIDER (CSP)	❖ 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) ❖ LexisNexis – API (Component) ❖ MaxMD – PKI ❖ Mastercard – API (Component) ❖ Persona – API (Full Service – In process)
HEALTH INFORMATION EXCHANGES (HIEs)	❖ HIEs connected to the Invitae Cures Gateway
CERTIFICATE ISSUERS	❖ EMR Direct (UDAP™ Tiered OAuth) ❖ MaxMD (UDAP™ Tiered OAuth)
IDENTITY BROKER	❖ Department of Health and Human Services NextGen XMS team (HHS XMS)
RELYING PARTY (RP)	❖ 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 FRAMEWORKS	❖ DirectTrust

	❖ Kantara Initiative
GOVERNMENT OBSERVERS	❖ The Centers for Medicare and Medicaid Services (CMS) ❖ The Office of the National Coordinator for Health Information Technology (ONC)

Appendix B. Acronym Table

Abbreviation	Meaning
AAL	Authenticator Assurance Level
API	Application Programming Interfaces
CSP	Credential Service Provider
DR	Disaster Recovery
EHR	Electronic Health Record
FHIR®	Fast Healthcare Interoperability Resources
HDO	Health Database Organization
HHS XMS	Department of Health and Human Services External User Management System
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HL7®	Health Level Seven International
IAL	Identity Assurance Level
IAS	Individual Access Services
IG	Implementation Guide
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
OIDC	OpenID Connect
PHA	Patient Health Application (also referred to as Client Application)

PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PoC	Proof of Concept
RP	Relying Party
SAML	Security Assertion Markup Language
TEFCA	Trusted Exchange Framework and Common Agreement
UAT	User Acceptance Test
UDAP™	Unified Data Access Profiles
URI	Uniform Resource Identifier
USCDI	United States Core Data for Interoperability
XID	External ID

Appendix C. Definitions Adopted and Used for the Proof of Concept (PoC)

PoC DEFINITIONS		
TERM	**NIST DEFINITION**	**PoC ADOPTED DEFINITION**
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. While common usage often assumes that the subscriber maintains the credential, these guidelines also use the term to refer to electronic records maintained by the CSP that establish binding between the subscriber's authenticator(s) and identity.	No Change – Adopting NIST Definition

Credential Service Provider (CSP) Synonyms: IdP	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use. Also stated within NIST-800-63-3: ● Notably, CSPs can be componentized and comprised of multiple and owned business entities. ● Accordingly, the term CSP will be inclusive of Registration Authority (RA) and Identity Manager (IM) functions.	The CSP is the collection of hardware, software, and operating personnel that create, sign, and issue credentials to Users. The credentials issued by the CSP are only issued to natural persons, not roles. The CSP is responsible for issuing and managing credentials including: • Identity proofing • Binding authenticators to an account and authenticating Users • Approving the issuance of all credentials • Maintenance of active web services that may support CSP discovery • Revocation of credentials • **Signing assertions of identity containing verified claims about the CSP's Users** • Generation and destruction of assertion signing keys • Establishing and maintaining the CSP system • Establishing and maintaining the Credential Practices Statement (CPS) A CSP carries the responsibilities of an RA by policy, however, a CSP may outsource ID proofing to an accredited RA. CSPs take on the responsibilities defined in NIST 800-63-3 for IAL, AAL, and FAL. When meeting these requirements, "IdP" may be another term used to describe this participant.

		In some cases, the PoC recognizes that the identity verification performed by CSPs may be relevant without an accompanying authentication event through a Verifier.
Data Holder Synonyms: resource owner; resource holder; relying party		A data holder is a type of Relying Party that possesses or manages data about Users and makes risk-based decisions concerning the release of the User's data. User's data is released when requested by an authenticated and authorized requestor. Data Holders are responsible for properly matching the User's identity to records that the Data Holder possesses.
Registration Authority (RA) Synonyms: Identity Proofing Component	A trusted entity that establishes and vouches for the identity or attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).	The registration authorities (RAs) collect and verify each User's identity and information that is to be entered into the User's CSP system. The RA performs its function in accordance with a Credential Practices Statement (CPS) or Registration Practices Statement (RPS) approved by a Trust Framework. The RA is responsible for: • The registration process • The identification and authentication (identity proofing) of identity evidence • Binding or facilitating the binding of authenticators by working with CSPs
Relying Party	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.	A Relying Party is an entity that relies on the validity of the binding of the User's identity attributes to an assertion signed by a CSP. The Relying Party uses a CSP's signed assertion to verify or

		establish the identity of the User. A Relying Party is responsible for deciding whether or how to check the validity of the assertion and the mechanisms used to verify the trust of the data contained in an assertion from a CSP. A Relying Party may use information in a certificate to determine the suitability of an assertion for a particular use. Relying parties may be User Client Applications, Data Holders or other participants that require the ability to discern trustworthiness of identity claims contained in an assertion of identity. Relying Parties should also be policy aware to ensure the assurance level defined in the assertion does not exceed the maximum level of assurance granted by a Trust Framework to the CSP, thereby ensuring the level of assurance at which a user has been authenticated is commensurate with the risk assumed by the Relying Party. The responsibility to make authorization and access control decisions lies solely with the Relying Party.
User Synonyms: applicant; subscriber; claimant	**Applicant:** A subject undergoing the processes of enrollment and identity proofing. **Subscriber:** A party who has received a credential or authenticator from a CSP. **Claimant:** A subject whose identity is to be verified using one or more authentication protocols.	A User is the natural person who has been: • Identity proofed by the CSP; • Issued an authenticator bound to the User's account; • Is represented in the assertions signed by the CSP, and;

		• Consents to the CSP sharing the User's data with other parties. User is analogous to the terms Applicant, Subscriber, and Claimant in NIST 800-63-3 as defined by this policy.
User Client Application Synonyms: PHA		A user client application is an application making protected resource requests on behalf of the User and with the User's authorization. The term "client" does not imply any particular implementation characteristics (e.g., whether the application executes on a server, a desktop, or other devices). The user client application may share information with a data holder to support the discovery of the User's CSP via UDAP™ Tiered OAuth in order to obtain trustworthy claims about the User or employ other mechanisms. In certain situations, user client applications that take on the responsibilities of authenticating Users and attesting to authenticated Users' identities, effectively take on the role and responsibilities of a CSP as defined by this policy.

Appendix D. Additional Definitions of Interest to the PoC

ADDITIONAL TERMS OF INTEREST TO THE PoC	
TERM	**NIST DEFINITION**
Assertion	A statement from a verifier to an RP that contains information about a subscriber. Assertions may also contain verified attributes.

Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
Authentication Factor	The three types of authentication factors are something you know, something you have, and something you are. Every authenticator has one or more authentication factors.
Authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a token.
Multi-Factor Authentication	An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Trust Anchor	A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g., in a public key certificate). A trust anchor may have name or policy constraints limiting its scope.
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

SOURCE: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Appendix E. Crosswalk of ONC, OIDC, USCDI Data Elements with FAST Patient Weighted Input

This crosswalk is a potential data set to identify a patient and improve match rates.

USCDI Name	Data Value from ONC Example in OIDC Format	OIDC Key	FAST Patient Weighted Input[7]
First Name	"Alice"	given_name	3 (if both)
Last Name	"Newman"	family_name	
Date of Birth	"1970-05-01"	birthdate	2
Current Address	{"street_address": "1357 Amber Dr", "locality": "Beaverton", "region": "OR", "postal_code": "97006", "country": "US"}	address	4 (any one of these or another identifier; at most 5 for two or more)
Email Address	*"alicenewman@example.com"*[8]	email	
Phone Number	"+1 (555) 777-1234"	phone_number	
Middle Name (Including Middle Initial)	"Jones"	middle_name	
Suffix	""	*suffix*	
Previous Name	"Alicia"	*previous_name*	
Sex (Assigned at Birth)	"female"	*sex_assigned_at_birth*	
Previous Address	{}	*previous_address*	
Phone Number Type	"mobile"	*phone_number_type*	

[7] Refer to the HL7® Interoperable Digital Identity and Patient Matching Implementation Guide (for additional details. NOTE: The May 2022 Ballot version of the IG is referenced in this white paper. Refer to the Publication History for updates.
[8] Italicized text did not yet exist for the ONC test patient and were therefore created for testing purposes.

Additional verifiable identifiers and other distinguishing demographic attributes, including insurance member identifier, SSN Last 4, identifiers from state and federal photo IDs, individual profile photo,[9] and unique patient identifiers established by health systems and other identity services (for example, the globally unique digital identifier in HL7®'s Interoperable Digital Identity and Patient Matching Implementation Guide) were discussed as other useful additions to the list above. Given that presence in USCDI is considered a prerequisite, it would be helpful to consider adding some or all of these to USCDI (along with the corresponding identifier assigner, when necessary) so that they may become candidates for future industry-wide patient matching recommendations. Given its high weighting (10) and privacy-aware requirements, the HL7® Implementation Guide's Digital Identifier designed for this purpose and for CSPs' implementation, like the participants in this PoC, could be helpful on its own if just one element could be added to USCDI.

The PoC then discussed various possible patient matching scenarios and what might be expected regarding the confidence level of matching in real world scenarios. For example, the healthcare industry will need to determine what happens if:

- Data from the CSP and the RP are a MATCH across all data elements.
- Data in the CSP is validated, but the data in the RP are a partial match.
- Not all required data elements are included; therefore, there is not enough information for the RP to provide the medical records.
- There is a false positive where the CSP has gone through the validation process, but the RP brings back data for the WRONG PERSON.
- There is a false positive where the CSP has validated but the RP cannot find the person.

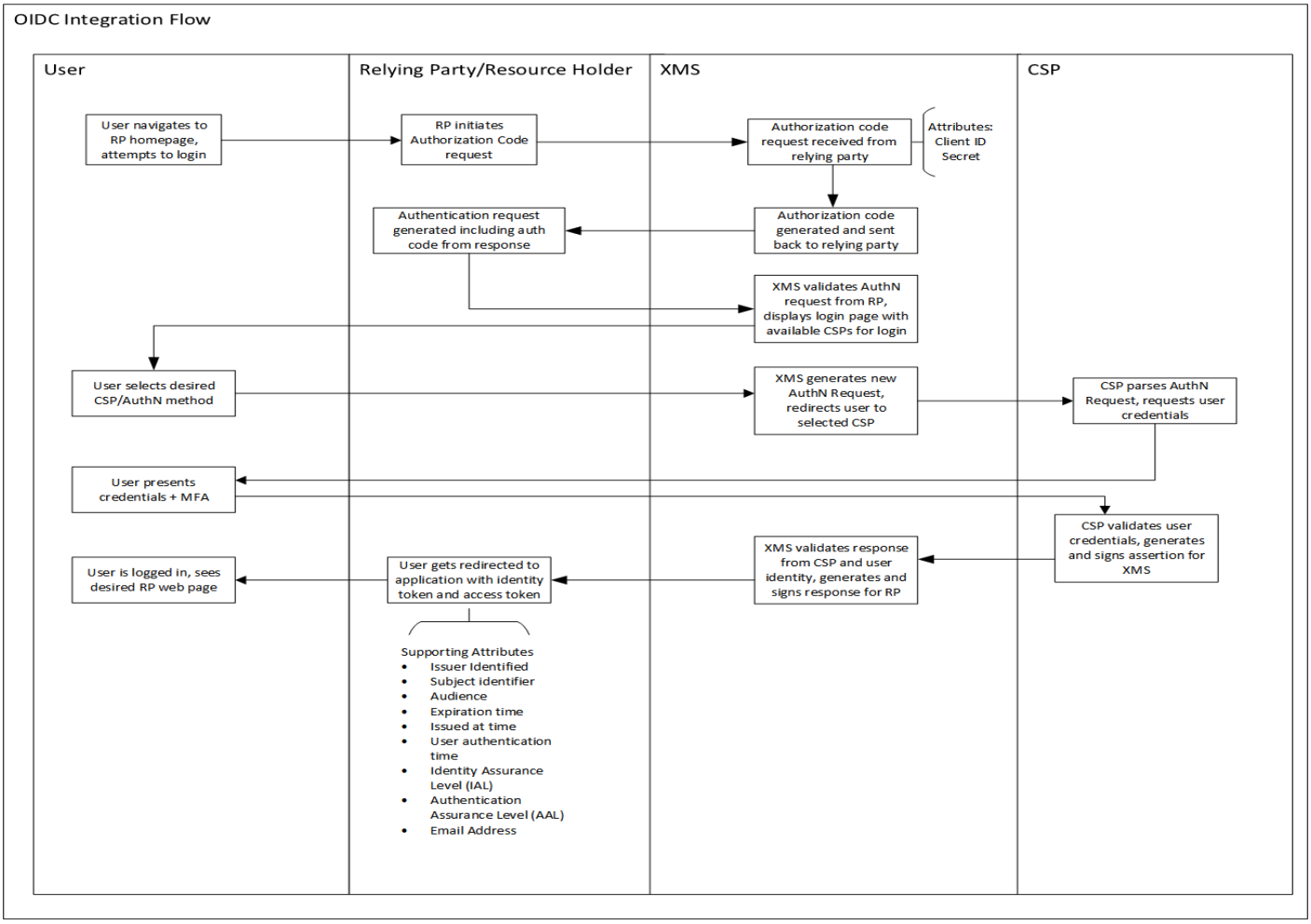
Expected results for each scenario are outlined below.

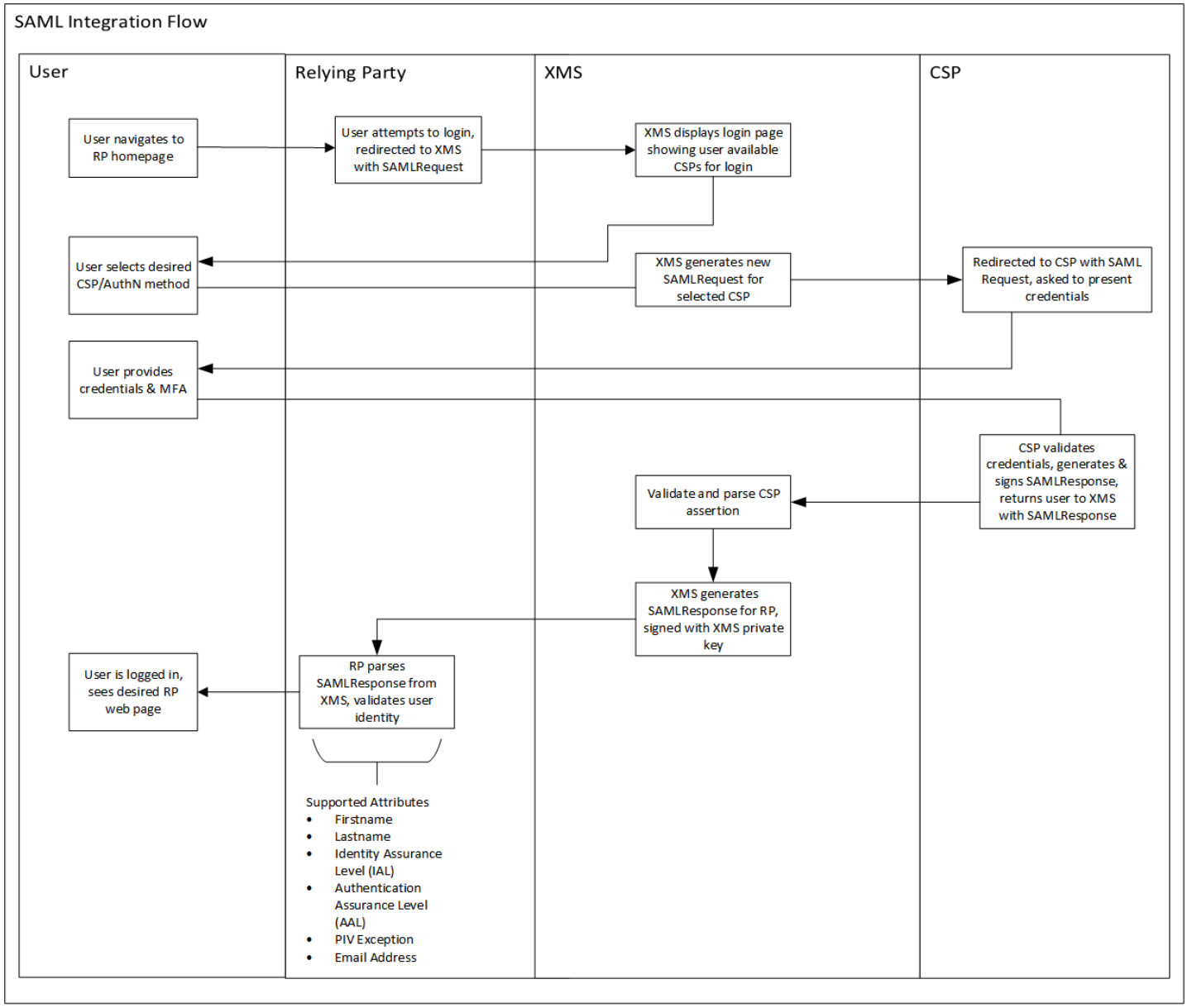
PATIENT MATCHING & DATA DEMOGRAPHICS			
	CSP DEMOGRAPHICS	**RP DEMOGRAPHICS**	**EXPECTED RESULTS**
SINGLE HIGH - CONFIDENCE MATCH	FN – Robert LN – Smith DOB – 1/1/1960 1357 Amber Dr 97006	FN – Robert LN – Smith DOB – 1/1/1960 1357 Amber Dr 97006	RP ***will*** provide the medical records of the patient because it matches on all the required fields and the application ***will*** accept those medical records since it's the right patient.
PARTIAL MATCH	FN – Robert LN – Smith DOB – 1/1/1960 1357 Amber Dr	FN – Roger LN – Smith DOB – 1/1/1960 1357 Amber Dr	RP ***will not*** provide the medical records of the patient. The claims may ***not*** match all the required fields,

[9] The FAST Identity Team's discussions about the use of biometrics in patient matching resulted in a recommendation for the use of a verified Individual Profile Photo as beneficial to matching. See the Guidance section of its HL7® Interoperable Digital Identity and Patient Matching Implementation Guide for additional information.

	97006	97006	insufficient input data provided, or claims match ***more than one*** health record.
NOT ENOUGH INFORMATION	FN – Robert LN – Smith DOB – 1/1/1960	FN – Robert LN – Smith DOB – 1/1/1960	RP ***will not*** provide the medical records of the patient because it ***does not include*** all the required fields.
WRONG PERSON	FN – Robert LN – Smith DOB – 1/1/1960 1357 Amber Dr 97006 Previous Name – Jones (not verified by CSP or shared in match request)	FN – Robert LN – Smith DOB – 1/1/1960 1357 Amber Dr 97006 Previous Name – Estrada	RP **will** provide the medical records of the patient because it matches on all the required fields ***but*** the application ***will not*** accept those medical records because the additional 'SHOULD' share data elements indicate this is ***not*** the right patient.
PERSON NOT FOUND	FN – Robert LN – Smith DOB – 1/1/1960 1357 Amber Dr 97006	FN – Not Found LN – Not Found DOB – Not Found Address – Not Found	RP ***will not*** provide the medical records of the patient because the patient ***is not found*** in the data holder's system.

Appendix F. HHS XMS Technical Flows (OIDC and SAML 2.0)




SAML Integration Flow
User
Relying Party
XMS
CSP
User navigates to RP homepage
User attempts to login, redirected to XMS with SAMLRequest
XMS displays login page showing user available CSPs for login
User selects desired CSP/AuthN method
XMS generates new SAMLRequest for selected CSP
Redirected to CSP with SAML Request, asked to present credentials
User provides credentials & MFA
CSP validates credentials, generates & signs SAMLResponse, returns user to XMS with SAMLResponse
Validate and parse CSP assertion
XMS generates SAMLResponse for RP, signed with XMS private key
User is logged in, sees desired RP web page
RP parses SAMLResponse from XMS, validates user identity
Supported Attributes
Firstname
Lastname
Identity Assurance Level (IAL)
Authentication Assurance Level (AAL)
PIV Exception
Email Address

Appendix G. Initial Minor's Identity and Personal Representative's Use Cases

Background

This is intended to capture the high-level healthcare use cases which are currently problematic to solve for minors and to aid in the conceptualization and execution of appropriate solutions. The CARIN Alliance would encourage feedback from the healthcare, patient, minor, and caregiver communities on whether this covers all the use cases associated with minors and HIPAA personal representatives. The use cases are captured in the standard agile AS A, I WANT, SO THAT format that will be familiar to any requirements analyst.

Definitions

Minor

A person under the age of 18. In some contexts, this may refer to a person within an age range, such as 13 to 17, which has been defined for the context. When used in use cases here, without further qualification, minor means both Legally and Situationally Emancipated Minors according to the following definitions.

Situationally Emancipated Minor

A minor who is granted the ability by state law to consent to certain types of health care services independent of any parental authority. Age ranges of minors and the types of treatment to which they may consent vary widely by state, as do the regulations regarding informing or engaging parental authorities after the fact.

Legally Emancipated Minor, or in common use 'Emancipated Minor'

A minor who is legally freed from the control of any parental authority. While all states allow legal emancipation, the rules for emancipation vary by state, but usually include such acts as marriage, military service, and economic self-sufficiency.

HIPAA Personal Representative, or Personal Representative

A person formally designated by an individual under 45 CFR 164.502(g) to exercise that individual's rights by proxy around uses and disclosures of that individual's health information.

Use Cases

Treatment

AS A Legally Emancipated Minor who is legally able to consent to all health care services

I WANT to be able to readily access and use those services

SO THAT I can get the health care treatment I need.

AS A Situationally Emancipated Minor who is legally able to consent to certain kinds of health care services

I WANT to be able to readily access and use those services

SO THAT I can get the health care treatment I need.

AS A Provider of healthcare services

I WANT to be able to readily identify and authorize Legally Emancipated Minors who are seeking services

SO THAT I can treat them.

AS A Provider of healthcare services

I WANT to be able to readily identify and authorize Situationally Emancipated Minors who are seeking services

SO THAT I can treat them.

Payment

AS A Legally Emancipated Minor

I WANT to be able to access any pertinent health care benefits I may have

SO THAT I can use those benefits to pay for my treatment.

AS A Situationally Emancipated Minor who is legally able to consent to certain kinds of health care services

I WANT to be able to access any pertinent health care benefits I may have for those services

SO THAT I can use those benefits to pay for my treatment.

AS A Provider of healthcare services

I WANT to be able to readily identify and then verify the health insurance benefits of a Legally Emancipated Minor

SO THAT I can charge the Legally Emancipated Minor and bill their health plan appropriately.

AS A Provider of healthcare services

I WANT to be able to readily identify and then verify the health insurance benefits of a Situationally Emancipated Minor as a health plan dependent

SO THAT I can charge the Situationally Emancipated Minor and bill their subscribing parental authority's health plan appropriately.

AS A Payer of healthcare services

I WANT to be able to readily identify and then provide verification of the health insurance benefits of a Legally Emancipated Minor

SO THAT I can honor my contract with them and accurately pay claims for covered charges.

AS A Payer of healthcare services

I WANT to be able to readily identify and then provide verification of the health insurance benefits of a Situationally Emancipated Minor under their parental authority's plan

SO THAT I can honor my contract with their subscribing parental authority and accurately pay claims for covered charges.

Information Access

AS A Legally Emancipated Minor

I WANT to be able to readily access my health care records from Providers and Payers

SO THAT I can use the records for my own purposes.

AS A Situationally Emancipated Minor

I WANT to be able to readily access my health care records from Providers and Payers for treatments to which I consented, and any related claims, without knowledge of my access by any parental authority

SO THAT I can use the records for my own purposes.

AS A HIPAA Personal Representative of Legally or Situationally Emancipated Minor,

I WANT to be able to access the Minor's health care records as permitted by my Personal Representative relationship with the Minor

SO THAT I may perform any duties required by my Personal Representative relationship with the Minor.

AS A Minor

I WANT to be able to authorize HIPAA Personal Representatives, when permitted by state and federal law, to act on my behalf with respect to access to my health records

SO THAT they may perform any duties permitted under our relationship.

AS A Provider or Payer

I WANT to be able to identify a Legally Emancipated Minor

SO THAT I may release them their records.

AS A Provider or Payer

I WANT to be able to identify a Situationally Emancipated Minor

SO THAT I may release them the records about treatments and claims to which they have consented.

AS A Provider or Payer

I WANT to be able to identify the Personal Representative of a Minor and grant them access to health records as permitted by their documented formal relationship with a Minor

SO THAT I may release the records allowed by that relationship to the Minor.

As a Provider or Payer

I WANT to limit access of a parental authority to the health records of a Situationally Emancipated Minor when necessary

SO THAT I am in compliance with all state and federal privacy laws.

AS A Provider or Payer

I WANT to be able to identify the Personal Representative of a Minor and grant them the ability to authorize access to the individual's health records to a third party as permitted by their documented formal relationship with a Minor

SO THAT I may release the records to a third party as allowed by that relationship to the Minor and authorized by the Personal Representative.