Building an Ecosystem of Trust in US Healthcare: Identity Federation and Trust Frameworks

Ryan Howells
Program Manager, CARIN Alliance
Principal, Leavitt Partners

Kyle Neuman
Director, Business Development
DirectTrust
How will consumers aggregate and share data in the future?

FTC

The CARIN Alliance

Multiple APIs

App #1  App #2  App #3  App #4  App #5

Consumer-Directed Exchange

API 1  API 2  API 3  API 4

HIPAA

HIPAA

The CARIN Alliance

Multiple APIs

App #1  App #2  App #3  App #4  App #5

Consumer-Directed Exchange

API 1  API 2  API 3  API 4

FTC

The CARIN Alliance

Multiple APIs

App #1  App #2  App #3  App #4  App #5

Consumer-Directed Exchange

API 1  API 2  API 3  API 4

The CARIN Alliance

Multiple APIs

App #1  App #2  App #3  App #4  App #5

Consumer-Directed Exchange

API 1  API 2  API 3  API 4

HIPAA
Our Vision

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

*Sample list of CARIN members. For a full list of the CARIN board and members go to: https://www.carinalliance.com/our-membership/carin-board-participants/*
### Consumer’s new “digital front door” to health care

<table>
<thead>
<tr>
<th>“The Key”</th>
<th>Digital Identity and Authentication for the Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What:</strong></td>
<td>Acceptance or creation of an IAL2 identity proofed digital credential</td>
</tr>
<tr>
<td><strong>Solution:</strong></td>
<td>Identity and access management (IAM) solution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>“The Door”</th>
<th>Standardized FHIR-based API data exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What:</strong></td>
<td>Standardized clinical, financial, administrative, and SDOH APIs</td>
</tr>
<tr>
<td><strong>Solution:</strong></td>
<td>Development of an API Gateway</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>“Community of Problem Solvers”</th>
<th>B2C health and health care applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What:</strong></td>
<td>Innovative applications solving a myriad of health care use cases</td>
</tr>
<tr>
<td><strong>Solution:</strong></td>
<td>A development portal that includes an automated application registration process</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>“Your Family”</th>
<th>Patients, Members, Caregivers, and others</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What:</strong></td>
<td>Consumers consenting to when, where, and how they want to share their data to achieve their goals</td>
</tr>
<tr>
<td><strong>Solution:</strong></td>
<td>An individual proactive, informed, and (ideally) federated consumer-directed, consent-based data sharing framework (As a start: CARIN’s Code of Conduct and Trust Framework)</td>
</tr>
</tbody>
</table>
Representative Attendee Organizations (30)


Focused on 5 issues:

1. **Authentication** – Multi-factor authentication / SMART / FIDO2 (AAL2)
2. **Identity** – GLEIF for organizational and NIST 800-63-3 (IAL2) for individual
3. **Trust & federation** – Open contractual principles with private sector certification bodies tied together with UDAP.org and OIDC
4. **Consent** – Informed, proactive user consent
5. **Matching** – Matching based on contractual trust principles and criteria
CMS Interoperability and Patient Access Final Rule

- **2019**
  - Draft 2 TEFCA released
  - CMS publishes Interoperability and Patient Access Proposed Rule
  - ONC publishes 21st Century Cures Act Proposed Rule

- **2018**
  - Draft TEFCA released
  - White House Executive Forum on Interoperability
  - CMS made data available to researchers through the Virtual Research Data Center

**2019**
- Providers are required to use 2015 Edition Certified EHR Technology
- Promoting Interoperability program requirements take effect for all providers
- March 2018
  - MyHealthEData and Blue Button 2.0 launched

**FALL 2020**
- Hospitals send event notifications regarding admission, discharge, and transfer to other providers

**LATE 2020**
- Public reporting of clinician or hospital data blocking and providers without digital contact info in NPPES

**JAN 1 2021**
- Patient Access API
  - Patient health care claims and clinical info made available through standards-based APIs for Medicare Advantage, Medicaid and CHIP FFS, Medicaid and CHIP managed care, and QHPs on the FFEs
- Provider Directory API
  - Payer Provider Directories made available through standards-based APIs

**JAN 1 2022**
- Payer-to-Payer data exchange
- Payers required to exchange patient USCDI data upon request

**APRIL 2022**
- Improved benefits coordination for dually eligible individuals

©2020 LEAVITT PARTNERS
Authentication
Fast IDentity Online (FIDO) (www.fidoalliance.org)

The FIDO protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user’s client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. The client’s private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user–friendly and secure action such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button.

The FIDO protocols are designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user’s device.
# Individual Identity

**Identity Assurance Level (IAL)**

NIST DIGITAL IDENTITY GUIDELINES = SP 800-63-3

- [https://pages.nist.gov/800-63-3/](https://pages.nist.gov/800-63-3/)

**Expected Outcomes of Identity Proofing:**

- Resolve, Validate, Verify

**Can Be Performed:**

- In-Person (Physically Present or Supervised Remote)
- Remote (Unsupervised)

<table>
<thead>
<tr>
<th>IAL1</th>
<th>IAL 1.??</th>
<th>IAL2</th>
<th>IAL3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity is self asserted</td>
<td>TBD</td>
<td><strong>Performed remote or in-person (physically present or supervised remote)</strong></td>
<td>In-Person ONLY (Physically present or Supervised Remote)</td>
</tr>
<tr>
<td>No validation or verification</td>
<td>TBD</td>
<td><strong>Identity evidence is collected, confirmed as being authentic by a CSP</strong></td>
<td>More identity evidence required</td>
</tr>
<tr>
<td>No verification</td>
<td>TBD</td>
<td><strong>Strong verification process to ensure that the identity evidence belongs to the subject</strong></td>
<td>Superior verification process that the identity evidence belongs to the subject</td>
</tr>
<tr>
<td>Address* confirmation not required</td>
<td>TBD</td>
<td><strong>Address is confirmed via enrollment code</strong></td>
<td>Postal address confirmation via mail return receipt, inspection of address on identity evidence</td>
</tr>
</tbody>
</table>

©2020 LEAVITT PARTNERS
Organizational Identity
Who is Global Legal Entity Identifier Foundation?

- GLEIF is a not-for-profit Swiss foundation, founded by the Financial Stability Board (FSB).
- GLEIF is overseen by 71 regulators (7 from the U.S.) and 19 observers in the Regulatory Oversight Committee (LEI ROC) from 50 countries.
- GLEIF Board has 16 independent directors.

Partners for LEI issuing (LOUs)
36 and growing

Issued LEIs to date
> 1,700,000
Organizational Identity
Legal Entity Identifier (LEI)

LEI is the linchpin that connects the dots across the universe of entity identification in the digital age

• 20-digit, alpha-numeric open-source code based on the ISO 17442 standard developed by the ISO that’s digitally signed (e.g., API, PKI, verifiable credentials)

• LEI records include basic information on the legal entity, including its name, address and legal form

• Ownership structure: Who’s who, who owns whom?

• Applicable to financial and non-financial companies, funds, trusts partnerships and governmental organizations

• Born out of the 2008 financial crisis, in response to the need for financial institutions to quickly and accurately identify the parties involved in financial transactions
Organizational Identity
The Role of the LEI Issuers

- LEI issuers – also referred to as Local Operating Units (LOUs) – supply registration, renewal and other services, and act as the primary interface for legal entities wishing to obtain an LEI.
Federation and Trust
A Person-Centric Approach to Health Data
Federation and Trust
Have We Seen This Problem Before?
Federation and Trust
The Current State of Identity

Current State

- Member → Payer
- Member → Provider
- Member → Other Relying Party
- Payer → Provider
- Payer → Other Relying Party
- Provider → Other Relying Party

Risk
Unmanaged or unknown risk that fluctuates between each identity provider

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

Technical Interoperability
Technical interoperability achieved by working with each external entity independently

Future State

- Member → Payer
- Member → Provider
- Member → Other Relying Party
- Payer → Trust Framework
- Payer → Other Relying Party
- Provider → Trust Framework
- Provider → Other Relying Party
- Other Relying Party → Trust Framework
- Other Relying Party → Other Relying Party

Trust Framework
33.3%

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

Technical Interoperability achieved by working with each external entity independently
Federation and Trust
Federating Trust is What a Trust Framework Does

Current Approach

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

Trust Framework Approach

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

IDENTITY CREDENTIALS IN PHYSICAL WORLD VS. DIGITAL WORLD

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

The challenge is that sharing everything on your driver’s license for every use case when you are sharing your identity with a relying party often results in overinformation of information. Creating a digital identity credential can help in avoiding oversharing by allowing individuals to only share the specific identity evidence needed to fulfill a specific use case.

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

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

https://www.carinalliance.com/our-work/digitalidentity/
Federation and Trust
Our approach to create a volunteer Trusted Federated Identity Ecosystem

Digital Federated Trust Agreement: Content Oversight Board

Contractual language that links each of the trust framework organizations together and outlines the standards, policies, conformance, and contractual terms for how relying parties can trust ID providers across trust frameworks; the content board will oversee the content for the federated trust agreement.

Trust Framework organizations (Certifiers)

Third-party organizations who certify the legal, policy, and technical aspects of the products being provided by identity and authentication providers. Organizations such as: DirectTrust, Kantara, SAFE Identity, DIACC, FIDO, and others.

Identity Providers (Issuers)

Identity & authentication providers or issuers who provide organizational or individual identity products, services, & credentials at an NIST IAL2 / AAL2 level or higher. These identity providers (e.g., IDEMIA, ID.me, etc.) may use technologies such as Open ID Connect/APIs or PKI.

Focus is on policy equivalency across trust frameworks

Relying Parties

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

To access the Digital ID and Federation whitepaper, go to: CARINAlliance.com and select Our Work → Digital Identity → Download our Digital Identity and Federation White Paper
NextGen XMS – Capabilities

NextGen XMS is a scalable, cloud-based solution that allows OpDivs to focus on their mission; and takes into consideration:
• Alignment with Digital Identity guidelines, ICAM and Cloud modernization efforts
• Security and compliance with federal standards (NIST, OMB, HHS EPLC requirements, etc.)
• Identity and Access Governance and delegated administration model
• Enterprise service that can secure access to external HHS applications
• Centralized platform that is flexible to integrate with third-party providers and services

### Capabilities & Benefits

<table>
<thead>
<tr>
<th>Secure Access:</th>
<th>Allows external users to access protected applications using credentials issued by the General Services Administration’s (GSA’s) Login.gov or via other agency’s PIV/CAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST 800-63-3 Compliance:</td>
<td>IAL1, IAL2, and IAL3, and  AAL2 and AAL3</td>
</tr>
<tr>
<td>Identity Proofing/Delegated Proofing:</td>
<td>Remote ID proofing using Login.gov; and delegated proofing for users that affiliate with an organization that’s managed within NextGen XMS.</td>
</tr>
<tr>
<td>Organization Affiliation:</td>
<td>Ability to create organizations and manage affiliations to those organizations within NextGen XMS</td>
</tr>
<tr>
<td>Access Requests/Approvals:</td>
<td>Configurable access request framework for an application</td>
</tr>
<tr>
<td>Organization Relationship Management:</td>
<td>Ability to create organizations and manage affiliations to those organizations</td>
</tr>
<tr>
<td>Accredited Platform and Helpdesk:</td>
<td>NextGen ATO in place which includes Login.gov; no impact to integrated application’s ATO, only ISA/MOU required</td>
</tr>
</tbody>
</table>
Users have one of two options for authenticating into XMS (other IdPs who are certified IAL2+ may be added later):

- Login.gov credentials:

- PIV/CAC credentials:
NextGen XMS Walkthrough – Logging In via Login.gov or PIV/CAC

Users will be redirected to Login.gov’s landing page to enter their credentials and second factor of authentication:

Users will be directed to register their PIV/CAC upon first-time log in to show ownership of account:
Federation and Trust
What the CARIN Alliance is doing to help federate trust

• Three Primary Documents:
  a) Federated Trust Agreement – Draft Contract
     ▪ Contract Terms for Trust Frameworks that sign on to the Federated Trust Agreement
  b) Federated Trust Agreement – Governance Policy (Charter)
     ▪ Policy which outlines how the Credential Policy and contract terms are governed, and maintained by the Federate Trust Agreement Organization
  c) Federated Trust Agreement – Credential Policy
     ▪ The credential policies of the Federated Trust Agreement
     ▪ Discussion Questions:
       o Are these the right minimum standards for a CARIN-approved Trust Framework (i.e., the standards Trust Frameworks that would sign on to the Federated Trust Agreement maintain)?
       o What sections do we need to add to this for it to apply across Trust Frameworks (i.e., the policies for the Trust Framework Agreement)? Should they be included in this document or a separate one?

• Next Steps:
  • Initial draft of these three documents will be complete in Q3 2021 for industry feedback
  • Initial pilot of a federated identity ecosystem between an application, payer(s), provider(s), and maybe others will begin in Q4 2021
How can we pull the digital identity components together?

July 1st – Patient Access APIs

Requirement: Member needs to be provisioned by the primary data holder

- **Member portal-based**: Member is provisioned by the data holder’s portal and the app uses the UN/PW via SMART
- **PREFERRED**: Member IdP-based: Member is provisioned by the data holder’s NIST 800-63 IAL2 IdP that’s been certified by an approved trust framework organization and the app uses the UN/PW via SMART

January 1st – Payer to Payer APIs

Requirement: Member needs to be provisioned by the primary data holder and the secondary data holder needs to accept the primary data holder’s user provisioning event including an indication of the member’s consent and the primary data holder’s organizational identity provisioning event

- **Member Portal-based**: Member is provisioned by the data holder’s portal and the app uses the UN/PW via SMART
- **PREFERRED**: Member IdP-based: Member is provisioned by the data holder’s NIST 800-63 IAL2 IdP that’s been certified by an approved trust framework organization and the app uses the UN/PW via SMART
- **Organizational Identity**: Organization gets a Legal Entity Identifier (LEI) from a Legal Operating Unit (LOU) that is part of GLEIF or use Open Corporates.
- **Digital Federation Agreement**: CARIN’s tiger team work to contractually provide equivalency across trust framework organizations so IdPs and relying parties can establish trust across the ecosystem
Q4 2021 / Q1 2022 Digital Identity Federation Pilot

How to prepare:

**Applications:** Ensure you are partnered with an IdP/CSP that issues IAL2 digital credentials (e.g., ID.me, Login.gov, Mastercard, Lexis Nexis, ZenKey, Experian, etc.)

**Health Plans:** Will you be an IdP or relying party?

**Providers:** Do you have a stand-alone IdP that is separate from your core EHR system? If not, can you get one?

**IdPs/CSPs:** Get certified with Kantara (API/OIDC) or DirectTrust/SAFE Identity (PKI)

**Relying Parties:** What questions do you need to get answered internally before you can participate in the pilot?

**Trust Framework:** Participate on our tiger team

**HHS XMS is an identity federation broker tool that allows for individuals to choose to log in by choosing from multiple CSPs that have been certified by a trust framework organization. It will feature prominently in the pilot.**
Questions

Presenters and Contact Information

Kyle Neuman
Managing Director, Safe Identity
Kyle.Neuman@makeidentitysafe.com

Ryan Howells
Program Manager, CARIN Alliance
Ryan.Howells@leavittpartners.com

@carinalliance | www.carinalliance.com | HL7.org/CARIN
https://www.carinalliance.com/our-work/digitalidentity/
The Authentication and Access Management services are supported via the NextGen External User Management System (XMS) across the external, non-HHS user community.

NextGen XMS Services:

- Authentication Services\(^1\)
- Identity, Account, and Entity Management Services\(^2\)
- Data Services\(^3\)

\(^1\) Simplified Sign-On & Federation Capabilities
\(^2\) Application Account and Entity Linking Capabilities
\(^3\) Reporting and Auditing Capabilities
From the Request Status tab, all users can view and manage their submitted requests:

**REQUEST STATUS**
View and manage your submitted requests.

**Search Requests**
- Status: - Select -
- Request Type: - Select -
- Keyword

**My Requests**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Request Type</th>
<th>Date Submitted</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization 3</td>
<td>Organization Registration</td>
<td>09/22/2020</td>
<td>PENDING</td>
<td>VIEW</td>
</tr>
<tr>
<td>Application 1</td>
<td>Application Access</td>
<td>09/14/2020</td>
<td>EXPIRED</td>
<td>VIEW</td>
</tr>
<tr>
<td>Organization 2</td>
<td>Admin Affiliation</td>
<td>09/02/2020</td>
<td>APPROVED</td>
<td>VIEW</td>
</tr>
<tr>
<td>Organization 1</td>
<td>Member Affiliation</td>
<td>07/24/2020</td>
<td>DENIED</td>
<td>VIEW</td>
</tr>
</tbody>
</table>

**REQUEST DETAILS:**
- Application: Application 1
- Request Type: Application Access
- Date: 09/14/2020
- Status: EXPIRED

**REQUEST CANCELLATION:**
- Organization: Organization 5
- Request Type: Organization Registration
- Date: 09/22/2020
- Status: PENDING
- Federal Sponsor Name: XMS Test
- Federal Sponsor Email: xms.test@hhs.gov
- Business Justification: Creating an organization in XMS