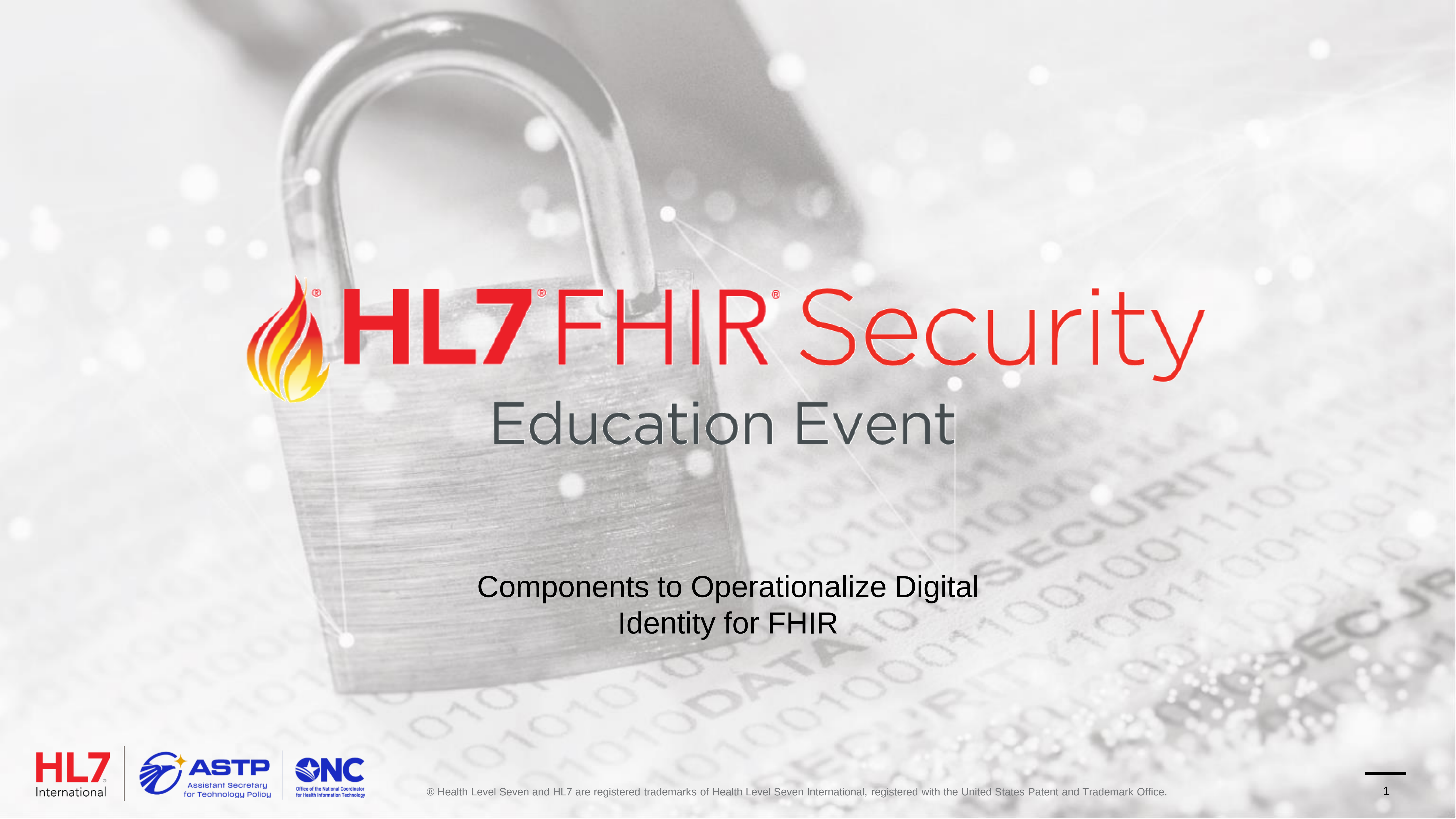


# HL7® FHIR® Security

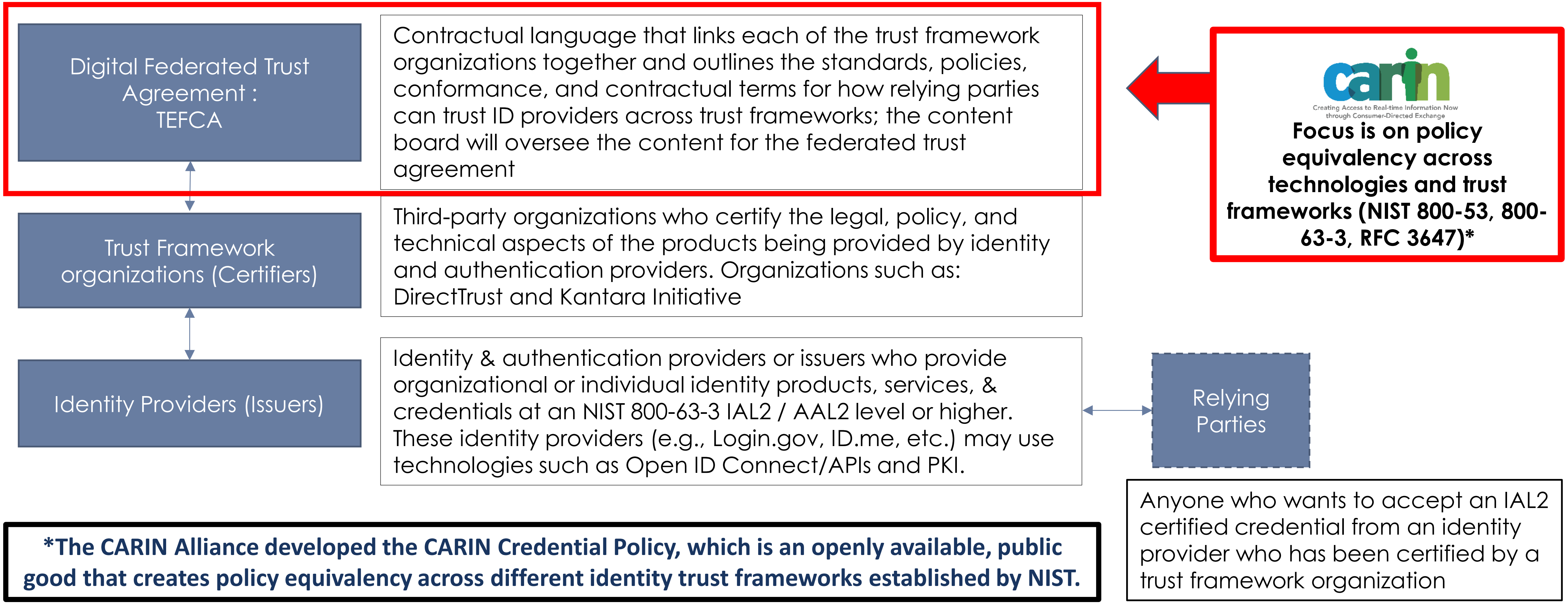
## Education Event

Components to Operationalize Digital Identity for FHIR

# CARIN / TEFCA Digital Identity Timeline

- **August 2017**: We first recommended to ONC they adopt the NIST 800-63-3 IAL2 guidelines
- **January 2018, April 2019, and January 2022**: First, Second, and Final versions of TEFCA recommended the adoption of a NIST 800-63-3 IAL2 digital credential
- **June 2019**: CARIN Digital Identity Summit in DC
- **December 2020**: CARIN released our whitepaper discussing how we could implement digital identity federation
- **January 2022**: CARIN launched the Healthcare Digital Identity Federation PoC with HHS, CMS, and ONC
- **June 2022**: The IAS Exchange Purpose Implementation SOP recommended the approach we discussed in our 2020 whitepaper
- **July 2022**: CARIN commented on changes to the IAS Exchange Purpose SOP
- **September 2022** : The final IAS Exchange Purpose Implementation SOP incorporated the changes CARIN recommended in July and mandated a response from TEFCA network participants when an IAS provider follows the IAS SOP
- **March 2023**: CARIN published the PoC Report and CARIN Credential Policy
- **July 2023**: Carequality published their patient request identity verification policy as part of their Technical Trust Policy that requires an IAL2 credential for patient access
- **December 2023**: CARIN published a Best Practice Recommendations for HL7® FHIR® Based Deployment
- **July 2024**: ONC released the HTI-2 proposed rule, which incorporated CARIN's recommendation to support multi-factor authentication

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



Digital Federated Trust Agreement : TEFCA

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 and Kantara Initiative

Identity Providers (Issuers)

Identity & authentication providers or issuers who provide organizational or individual identity products, services, & credentials at an NIST 800-63-3 IAL2 / AAL2 level or higher. These identity providers (e.g., Login.gov, ID.me, etc.) may use technologies such as Open ID Connect/APIs and PKI.

carin

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

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

Relying Parties

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

***The CARIN Alliance developed the CARIN Credential Policy, which is an openly available, public good that creates policy equivalency across different identity trust frameworks established by NIST.**

# CARIN / HHS Digital Identity Federation Proof of Concept

**OBJECTIVE**

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

- The CARIN Alliance partnered with 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), the HL7® FAST Digital Identity Tiger Team, and 25 other public/private sector stakeholders to develop a healthcare digital identity federation and API-based health information exchange Proof of Concept (PoC).
- The PoC tested four uses cases:
  - ❖ CSP Standalone/Interoperability (Multiple Relying Parties)
  - ❖ HIE Workflow (Non-FHIR APIs Flow)
  - ❖ HHS XMS (Multiple CSPs)
  - ❖ CSP with UDAP (HL7® FHIR® Network Transactions)
- Once implemented in production, the PoC's work eliminates the need to create separate "portal" accounts for data holders.

**To access the Healthcare Digital Identity Federation Proof of Concept Report and its lessons learned, go to: CARINAlliance.com and select Online Patient Registration → Digital Identity → Proof of Concept Final Report**

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

# Goals of The CARIN Identity Federation WG

**Goal:** Develop a set of policy and/or regulatory requirements we can provide to ONC, CMS, and the RCE on how to facilitate patient mediated exchange with both TEFCA and any future CMS/ONC rules

**Step 1:** Define all components necessary to implement patient mediated exchange over FHIR
**Step 2:** Define the problems inhibiting digital identity federation to submit IAS queries and get responses to queries as an initial use case
**Step 3:** Develop recommendations to each problem
**Step 4:** Develop and address technology, policy, and budget barriers and benefits.

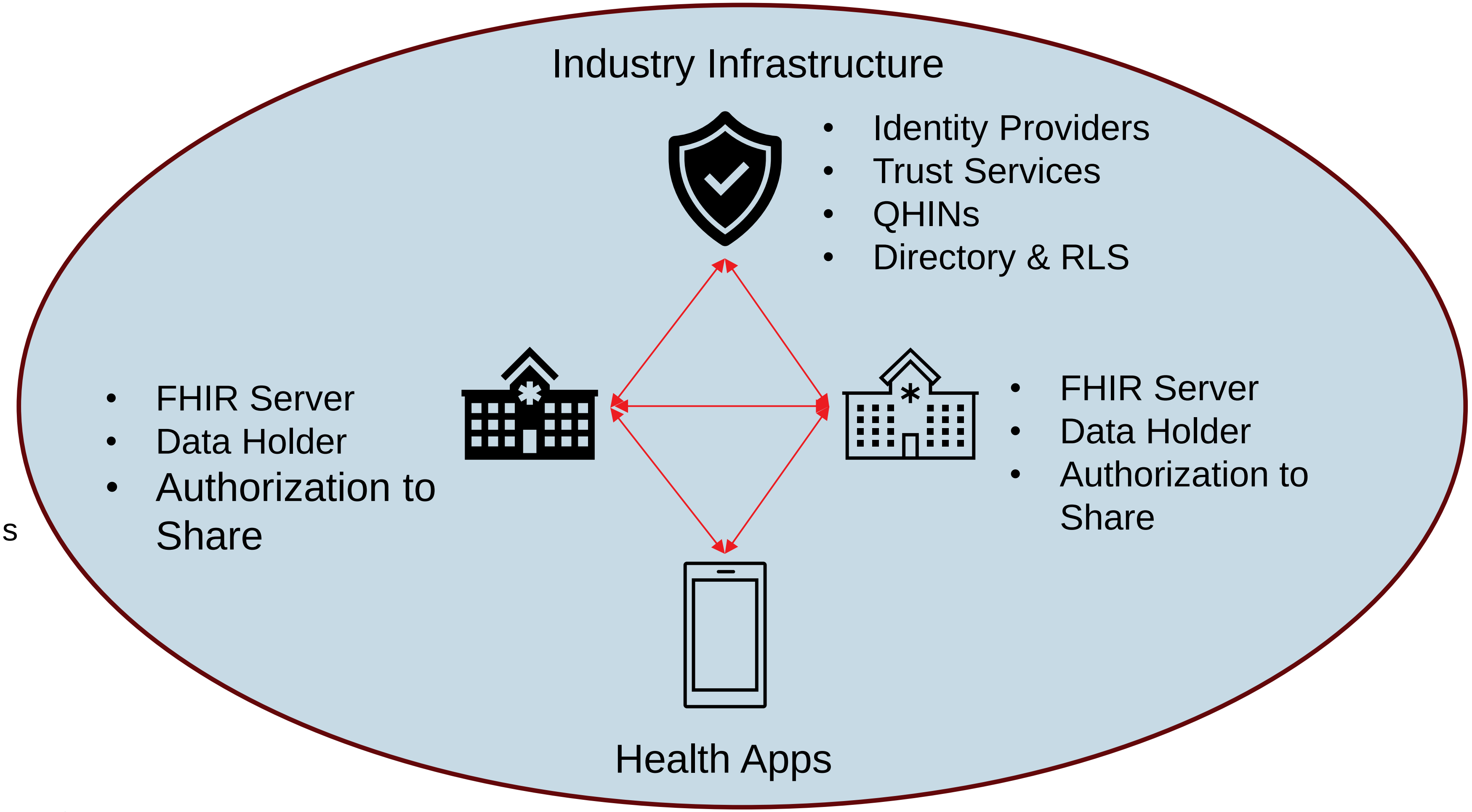
# What Components Do We Need?

| Capability Category (Ordered in Increasing in Footprint) | Individual Components |
|---|---|
| Standard protocols for exchanging data at individual systems | ● FHIR<br>● Authorization protocols for segmenting data and determining sharing privileges<br>● Mechanism for tracking disclosures (when was data shared, with whom, and who authorized it)<br>● Workflow automation capabilities that can operationalize the autonomy of FHIR-based exchange |
| Industry infrastructure<br>*Enables FHIR-based Exchange to scale technically | ● Technical trust mechanism to promote scale<br>● Record locator service<br>● Directory service or other industry-wide mechanism for knowing who is party to the agreement(s) mentioned above |
| Governance: Nationwide Regulatory, Legal and Procedural Considerations<br>*Authorizes and Governs Industry Infrastructure | ● IAL2 & AAL2 + operational controls<br>● RCE SOPs<br>● Contractual agreements handling liability and rules of the road<br>● Regulatory considerations for easing the regulatory risk of a false positive match (e.g. safe harbor if minimum matching efforts were made in good faith)<br>● Consistency in collecting demographics used to match patients across systems |

# How Do These Components Fit Together?

Governance &
Administration

- Regulations
- Contracts
- Procedural Controls



Industry Infrastructure

- Identity Providers
- Trust Services
- QHINs
- Directory & RLS

- FHIR Server
- Data Holder
- Authorization to Share

- FHIR Server
- Data Holder
- Authorization to Share

Health Apps

# Areas of Focus

| Capability Category (Ordered in Increasing in Footprint) | Individual Components |
|---|---|
| Standard protocols for exchanging data at individual systems | • FHIR<br>• Authorization protocols for segmenting data and determining sharing privileges<br>• Mechanism for tracking disclosures (when was data shared, with whom, and who authorized it)<br>• Workflow automation capabilities that can operationalize the autonomy of FHIR-based exchange |
| Industry infrastructure<br>*Enables FHIR-based Exchange to scale technically | • **Technical trust mechanism to promote scale**<br>• Record locator service<br>• Directory service or other industry-wide mechanism for knowing who is party to the agreement(s) mentioned above |
| Governance: Nationwide Regulatory, Legal and Procedural Considerations<br>*Authorizes and Governs Industry Infrastructure | • IAL2 & AAL2 + operational controls<br>• RCE SOPs<br>• Contractual agreements handling liability and rules of the road<br>• **Regulatory considerations for easing the regulatory risk of a false positive match (e.g. safe harbor if minimum matching efforts were made in good faith)**<br>• **Consistency in collecting demographics used to match patients across systems** |