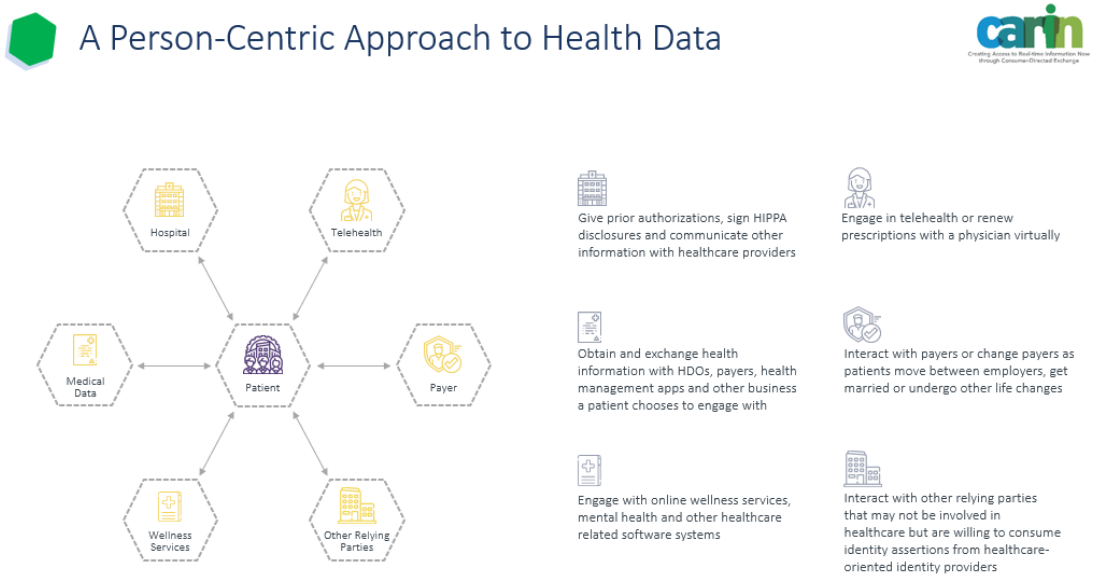
Identity Federation and Trust Framework – Overview

Background

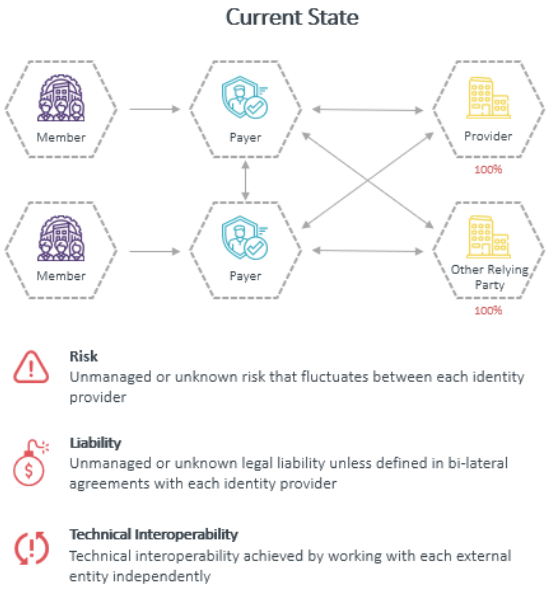
- During the Digital Identity Summit on June 4, 2019, CARIN focused on five issues:
  - **Authentication** – Multi-factor authentication / SMART / FIDO2 (AAL2)
  - **Identity** – GLEIF for organizational and NIST 800-63-3 (IAL2) for individual
  - **Trust & Federation** – Open contractual principles with private sector certification bodies tied together with UDAP.org and OIDC
  - **Consent** – Informed, proactive user consent
  - **Matching** – Matching based on contractual trust principles and criteria
- As of January 1, 2022, payers will be required to exchange patient USCDI data upon request. Payers are evaluating two ways to make the payer-to-payer exchange work:
  - DaVinci is considering using the current payer as the one who goes and gets the information from the previous payer (a business-to-business exchange under HIPAA). This would require an agreement to send information across payers.
  - The other approach is patient API using existing infrastructure. If a consumer is able to prove their identity once in an app, the ID proofing event makes it easier to do matching capability on the back end. This appears to be the approach payers are primarily moving towards.



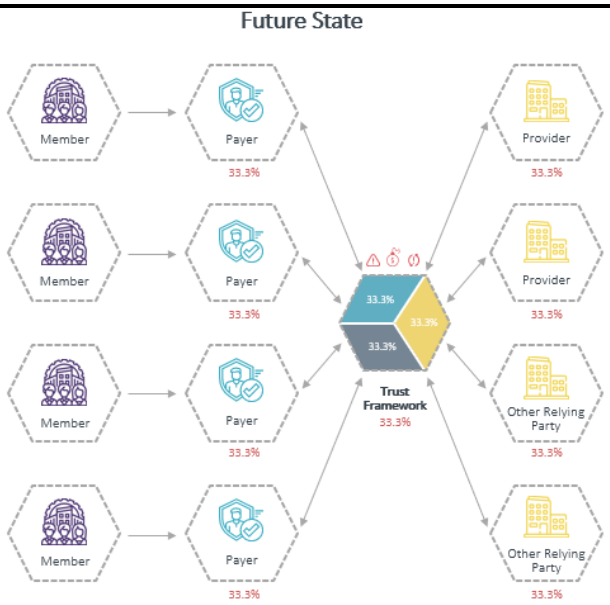
  - A patient centric approach to health data flips the model on its head. The consumer is in control and uses their federated identity among the different relying parties. However, there then needs to be a way to establish trust where the patient's identity can be trusted by the multiple relying parties that did not perform the identity proofing on their own. This is where trust framework organizations come in.

What is a Trust Framework and Why Is It Important?

- The current state of identity is point to point federation:

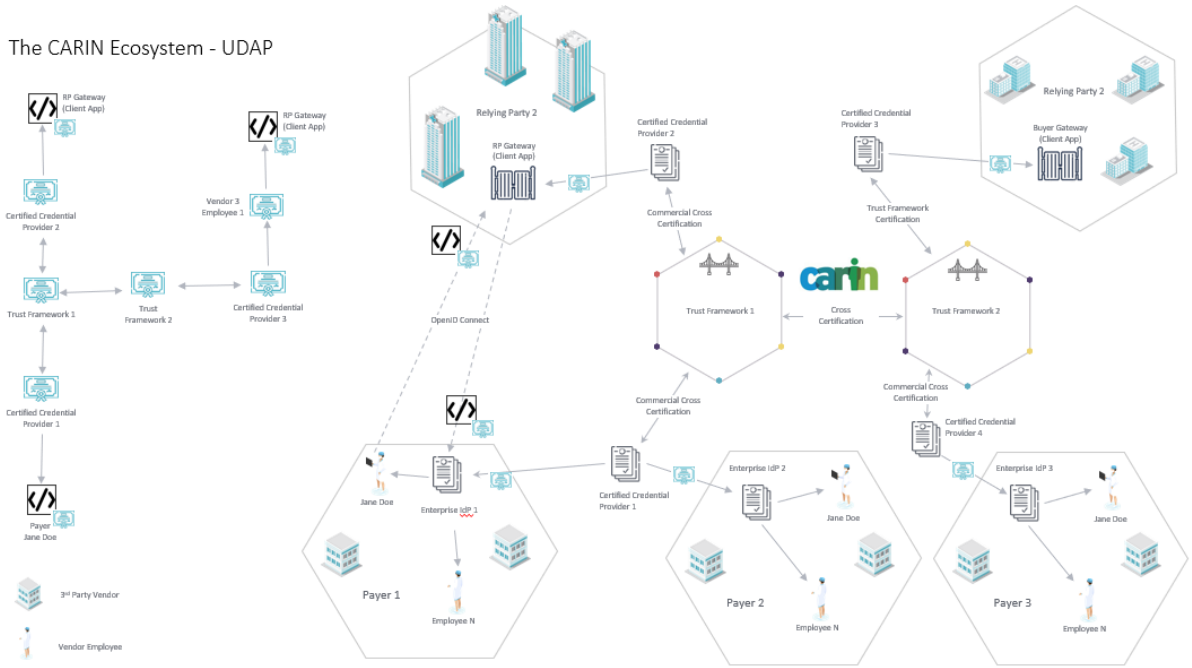


  - It is the responsibility of the two parties involved to make federation happen. This is not scalable. In a point-to-point approach, if a payer wants to exchange data with a provider/relying party, they would need to talk directly with one another.
  - This risk and liability associated with relying on an external identity credential must be negotiated individually between each pair of point-to-point federations, thus making liability inconsistent or undefined between parties. 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 they are relying on the assertion with no way to recover in the event that the IdP fails to properly manage the identity. With a trust framework, the liability is shared among all participants in a way that is consistent with the responsibilities they take on as a participant in the trust framework.
- Trust frameworks already exist today: Visa, Mastercard, the CA/Browser Forum, and Discover are a few examples.
  - Healthcare also already has trust frameworks: SAFE Identity, Kantara Initiative, DirectTrust, Carequality.
    - These frameworks have different audiences and CARIN is addressing how these different frameworks can have interoperability.
    - The future state of trust frameworks:



How It All Comes Together

- The below example illustrates the Ecosystem (UDAP):
  - Jane Doe is a member of payer one and wants to access an app elsewhere (a relying party such as a wellness app or an electronic health records system).
  - Jane Doe goes directly to this app to request access. The app (relying party) will need to determine who she is. In order for the app to find Jane Doe's identity provider, the app may use a directory of IdPs or some other function to locate Jane Doe's IdP (payer one). In the case of B2B interactions where Jane Doe is an employee of payer one, the app could use her work email to submit a query to her employer (payer one). In either case, once a query is sent to payer one IdP, Payer one IdP asks Jane whether she approves data sharing with the app and provides a list of claims it will share with the app that Jane Doe is trying to access. Jane approves the claims to be sent to the client app and then authenticates to the payer one IdP to prove it really is Jane Doe authorizing the claims. Payer one then redirects Jane Doe back to the app and includes an assertion signed by the payer one IdP that Jane Doe's browser will automatically provide the app (relying party). This is a typical OAuth flow.
  - In this scenario, we now have a relying party and a payer who have never communicated before able to exchange assertions. But, there remains the question of how to establish trust between the parties – this is where the trust framework comes in. The trust framework certifies a number of certificate authorities and IdPs. The certificate authorities issue certificates to IdPs which communicate the level of trust of the IdP. The certificates are used by the IdP to digitally sign assertions containing information about the IdPs subscribers (e.g., Jane Doe) and the level of assurance the subscriber has been authenticated at. This process is called tiered OAuth and allows the ecosystem to scale by making use of the UDAP protocol.
  - Multiple certificate authorities and IdPs in the trust framework also create competition that helps keep prices lower and increase innovation among the participants.
  - The diagram below illustrates this process:


The CARIN Ecosystem - UDAP
RP Gateway (Client App)
Certified Credential Provider 2
Trust Framework 1
Certified Credential Provider 1
Payer Jane Doe
3rd Party Vendor
Vendor Employee
Trust Framework 2
RP Gateway (Client App)
Vendor 3 Employee 1
Certified Credential Provider 3
Relying Party 2
RP Gateway (Client App)
OpenID Connect
Jane Doe
Enterprise IdP 1
Employee N
Payer 1
Certified Credential Provider 2
Commercial Cross Certification
Trust Framework 1
Cross Certification
Commercial Cross Certification
Certified Credential Provider 1
Enterprise IdP 2
Jane Doe
Employee N
Payer 2
Certified Credential Provider 3
Trust Framework Certification
Trust Framework 2
Commercial Cross Certification
Certified Credential Provider 4
Enterprise IdP 3
Jane Doe
Employee N
Payer 3
Relying Party 2
Buyer Gateway (Client App)