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

Digital Identity and Federation in Health Care

OUR HEALTH CARE IDENTITY VISION

The 21st Century Cures Act, the ONC Cures Act Final Rule, and the CMS Interoperability and Patient Access rule have accelerated the ability for an individual to access their personal health information via an application of their choice by leveraging HL7® FHIR® Application Programming Interfaces or APIs. Currently, the use of SMART on FHIR® allows for an individual to use their provider or payer portal username and password to authenticate themselves and retrieve their personal health information. While the CARIN Alliance strongly endorses the current implementation of SMART on FHIR® by stakeholders in the health care ecosystem to ensure individuals have immediate access to their health information, we also want to advance a future vision for how we could as an industry digitally authenticate individuals in a trusted way without being tied to the creation of portal accounts, and then allow an individual to use that same trusted authentication event to access their health information across multiple payers and providers.

We envision an ecosystem where an individual voluntarily creates a digital identity credential[1] in an application of their choice, which they own, manage, and use to access their health information from any health care payer or provider in the country. In order to realize this ecosystem, we must ensure that people are who they claim to be (often referred to as "identity proofing") before they are granted access to data, and then deploy strategies to match individuals across systems using trusted identifiers so the right information can be shared with the right person at the right time. In other words, we first need to establish a trusted digital identity credential and then we need to federate that trust.

TODAY'S HEALTH CARE IDENTITY PROBLEM

As an example of today's identity problem, today most providers rely on some type of manual "intake" process that enters individual demographic information into a registration portal, which is customized based on the provider's unique preferences. As a result, many providers who may have the same health IT vendor still cannot effectively match patients. This is largely because patients don't interact with the health system on a regular basis, and so when their information is entered into one of these manual "intake" registration screens, it's almost immediately out of date with other information that may be in a provider's system at another location or at another time, even when the provider is part of an integrated system with the same health IT vendor. This scenario leads to a never-ending "patient matching" problem as providers try to match disparate information provided by individuals at various points in time across systems. The industry has created referential matching, enterprise master patient index numbers, and other solutions to try and link records to a single person. We call this process trying to establish an "organizational-centric" digital identity. When patients are attempting to aggregate their own health information across multiple disparate systems, this "organizational-centric" approach doesn't work – especially for those with chronic conditions and multiple provider portals.[2]

[1]A digital identity credential is defined as a credentialing service provider or issuer who confirms that an individual meets the requirements associated with the NIST 800-63-3 identity assurance level 2 (IAL2) requirements and is certified by a trust framework organization.

[2]For a patient's perspective on the difficulties multiple portals cause individuals with chronic conditions, please see https://morgangleason.com/2014/10/16/reflections-from-a-patient-ucsf-peds-by-the-bay-post/.

The only constant in health care is the individual enrolling in coverage or receiving care. Therefore, CARIN supports "person-centric" digital identity credentials, where an individual has a portable, high-assurance digital credential they can use to control when and how their personal information is shared across systems. The individual person becomes the "single source of truth," and regardless of whether the information is out of date, it's still unique to the individual and the individual can use that same digital identity credential whenever they log in to a new system.

We envision a world where:

- A person can create their own unique digital identity credential prior to or at the time when they choose a coverage type during open enrollment.
- That same digital identity credential could be used to access their benefit and coverage information, including their pharmacy, formulary, and prescription drug information, when they are scheduling an appointment with their physician or picking up prescriptions.
- The more than 296 million Americans who have some type of government or private sector coverage are not required to re-identify themselves when they visit a physician or hospital.[3]
- The 27.5 million Americans who do not currently have health care coverage or do not have a government issued identity could create their own digital identity credential to better coordinate their care.[4]

The CARIN Alliance seeks to advance an equitable and more efficient health care experience by allowing individuals the ability to create, manage, and use their own digital identity, and then voluntarily use that digital identity across multiple systems to provide a more seamless and robust experience for themselves and their families.

HOW IDENTITY FITS INTO THE CONSUMER'S NEW "DIGITAL FRONT DOOR" TO HEALTH CARE

The CARIN Alliance describes the new ecosystem and infrastructure needed for sharing data between consumers and data holders as a "digital front door." Identity is a central component to this digital front door to ensure the individual has equitable access to their personal health information. In the ecosystem, there are four primary actors illustrated below using the following metaphors:

THE KEY

Digital Identity and Authentication for the Organization, Application, and Individual
What: Creation or acceptance of an identity proofed digital identity credential that has been securely authenticated
Solution: **Consumer Identity and Access Management (CIAM) solution**

THE DOOR

Standardized FHIR-Based API Data Exchange
What: Standardized clinical, financial, administrative, and SDOH APIs
Solution: Development of an **API Gateway**

[3]Berchick, E. R., Barnett, J. C. & Upton, R.D. (2019). Health insurance coverage in the United States: 2019. Current population reports. Washington DC: US Government Printing Office. Available at: https://www.census.gov/library/publications/2019/demo/p60-267.html
[4]Ibid.

COMMUNITY OF PROBLEM SOLVERS

B2C Health and Health Care Applications
What: Innovative applications solving a myriad of health care use cases
Solution: An automated application registration process

YOUR FAMILY

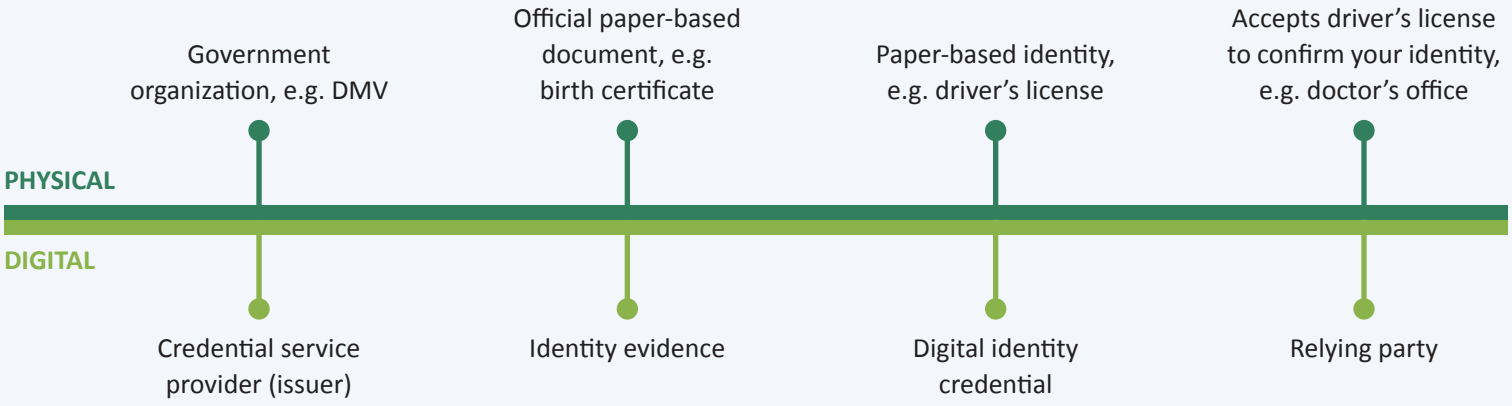
Patients, Members, Caregivers, and Others
What: Consumers consenting to when, where, and how they want to share their data to achieve their goals
Solution: An individual proactive, informed, and (ideally) federated consumer-directed, **consent-based data sharing framework** (As a start: CARIN's Code of Conduct and Trust Framework)

- The "key," which digitally identifies an individual, will provide a unique, digital credential so they can securely authenticate themselves to request, access, and share their own data with an application of their choice.
- The "door," or API Gateway, which controls the clinical, financial, and other data that is being shared using HL7® FHIR® APIs.
- The "community" of applications who are helping individuals solve a myriad of use cases within health care.
- The "family" of requestors: The related patients, members, caregivers and others who will seek access to data using an application of their choice.

This paper will focus primarily on the "key," or digital identity credential required to securely unlock the data being provided to the individual through a consent-based data sharing framework via the exchange of APIs using third-party applications.

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 oversharing 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.



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.[5] 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 our 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.

PRIMARY OBJECTIVE

Our primary objective is to replicate and then surpass the level of trust we have in the physical world in the digital world by following a similar process of creating trust in digital identity credentials. This would allow an individual to use a single digital identity credential when they authenticate themselves across multiple systems which allows for any health care organizations they interact with virtually to ensure their digital identity credential is valid, and helps streamline access to personal health information from multiple organizations, including health plans, providers, and applications.

[5]Digital identity is newer in health care but has gained significant transaction in other consumer-centric industries such as finance, consumer platforms, and telecom.

DIGITAL IDENTITY MODELS AND TRUST

There are multiple forms and technologies to create digital identity credentials which can be organized into three (3) different identity models: centralized, federated decentralized, and self-issued. (See inset for more information.) Of the three identity models above, a federated decentralized identity model is the most likely to scale in the current health care ecosystem. Over time, emerging identity models may gain more traction, such as self-issued identity, but as of now, the technology, standards, and policy framework are too immature to gain traction in health care and most other industries.

A federated decentralized identity model allows for flexibility and choice related to the digital identity. The CARIN Alliance is focused on developing a framework which allows an individual identity provider to be certified by an authorized trust framework organization or certifier to establish trust across relying parties. In an ideal world, this identity model would allow users to create a digital identity credential using a variety of technologies across different credentialing service providers (issuers). However, for a federated identity model to be implemented at scale, we must also federate trust in these digital identity credentials.

We noted previously that there are many credentialing service providers and trust framework organizations. Trust framework organizations create conditions for trust between the credential service providers (issuers) and relying parties which belong to them by conducting policy and technical conformance testing to ensure that a valid digital identity credential was issued in accordance with set standards (for example, the NIST 800-63-3 standards).[6] However, currently there is no mechanism to establish policy and standards equivalency between the trust framework organizations.[7] The CARIN Alliance is focused on developing a "federated trust framework model" which would create the needed equivalency.

We are drafting a federated trust agreement which outlines the technical, policy, legal and certification guidelines necessary to create trust so digital identity credentials can be used and accepted even when they are issued and certified by different trust framework organizations. We believe this will advance the ability to exchange personal health information across systems electronically.

IDENTITY MODELS

Centralized

A centralized identity model is one where a single organization or entity controls digital credentials and services. Banking services or centralized government identity approaches are prime examples of centralized identity models. Trust is established between the end user and the "siloed" identity provider. This trust must be repeated with each entity, just as one has to create multiple accounts to access financial services across multiple companies. Although technology companies provide services that mimic a federated identity model (see below), access to their own services requires authentication by the parent company utilizing a centralized identity model.

Federated Decentralized

In a federated decentralized identity model, the end user establishes identity information in one security domain to access another. The goal is to provide secure identities and attributes to be shared across trust boundaries between organizations, but also provide a measure of data portability. These systems have become increasingly common and are frequently used by technology companies; examples include "Sign in with...." For example, when a user uses their PayPal credentials through "Sign in with PayPal" to populate name and shipping address data when purchasing an item from Gap, they are benefiting from a federated identity model.

Self-Issued

Self-issued identity models, also known as self-sovereign identity, rely on the user's attestation of their own identity attributes. Third parties are not necessary for identity verification in this model. Blockchain has emerged as a technology method to underpin the backbone of a self-issued identity model by using distributed ledger technologies that rely on encryption using keys linked to a decentralized identifier. With self-issued identity, relying parties must trust the self-issued identity credential which could inhibit the proliferation of this approach.

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

[7]NIST 800-63-3 is a set of digital identity guidelines required for federal agencies implementing digital identity services. The guidelines define technical requirements related to identity proofing, authentication and federation. For more information, please visit: **https://pages.nist.gov/800-63-3/**.

FEDERATED TRUST AGREEMENT: THE PROCESS

CONSENSUS-BASED PROCESS

The CARIN Alliance has convened a small group of stake holder with equity in this work. The group is using a consensus-based process to develop a draft industry-level framework and set of open contractual terms and conditions which establish trusted policies to support federated digital identity.

Once drafted, the framework and terms and conditions will be refined and validated by CARIN Alliance members and broader industry stakeholders.

GUIDING PRINCIPLES

Our work on the CARIN Federated Trust Agreement is grounded in the principles outlined by National Strategy for Trusted Identities in Cyberspace (NSTIC)[8] in 2011 as part of their efforts to establish a common model for strong identity and authentication across the nation:

1. ***Identity solutions will be privacy-enhancing and voluntary.***
   Fair Information Practice Principles (FIPP) set forward by the FTC recommend the creation and adoption of policies and standards that preserve the capacity to engage in privacy-enhancing processes for uniquely identifying individuals. For personally identifiable data, industry agreed upon codes of conduct similar to what the CARIN Alliance code of conduct has established will help enforce common principles and best practices for data that are under FTC jurisdiction. Participation in services offered by issuers and accepted by relying parties should always be voluntary and provide value to the end user.
2. ***Identity solutions will be secure and resilient.***
   Security and resiliency are paramount to identity solutions and should be developed with auditable security processes – resistance to theft, tampering, counterfeiting and exploitation, phishing and credential compromise are elements to be strongly addressed. Detection of these breaches to minimize harm and restoring services after disruption.
3. ***Identity solutions will be interoperable.***
   Interoperability of identity solutions refers not only to technical processes, but also to policy-level interoperability.
4. ***Identity solutions will be cost-effective and easy to use.***
   Identity solutions which are not cost effective and/or difficult to use will not be widely accepted.

PRIMARY AND SECONDARY USE CASES

A federated trust agreement has multiple use cases in the health care setting. Our primary, and the most obvious, use case is for the consumer to be able to aggregate their health information from multiple payers and providers, especially in situations where an individual is managing a chronic condition. Once an individual user has been authenticated through a trusted identity provider, a digital trust agreement framework is helpful in authorizing reuse of the user's digital identity credential at multiple different relying party endpoints using appropriate technologies.

A secondary use case is for healthcare organizations to use the digital identity credential to securely verify the identity of someone requesting access to their health data online. Sorting out who is real and who is someone trying to leverage identity as an attack vector to get unauthorized access to health data is foundational to ensuring authorized access to health information online.

Another, although less frequent, use case is to facilitate the selective sharing of information. A federated trust agreement will facilitate selective information sharing by helping standardize extensions for authorization and delegation. Avoiding sharing the entire medical record reduces risk of a healthcare information breach and allows the individual control over when and how their information is shared. For example, it may not be relevant or necessary to share the entire medical record with a researcher, who may only be interested in blood tests and biopsy results.

[8]The White House. (2011). National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

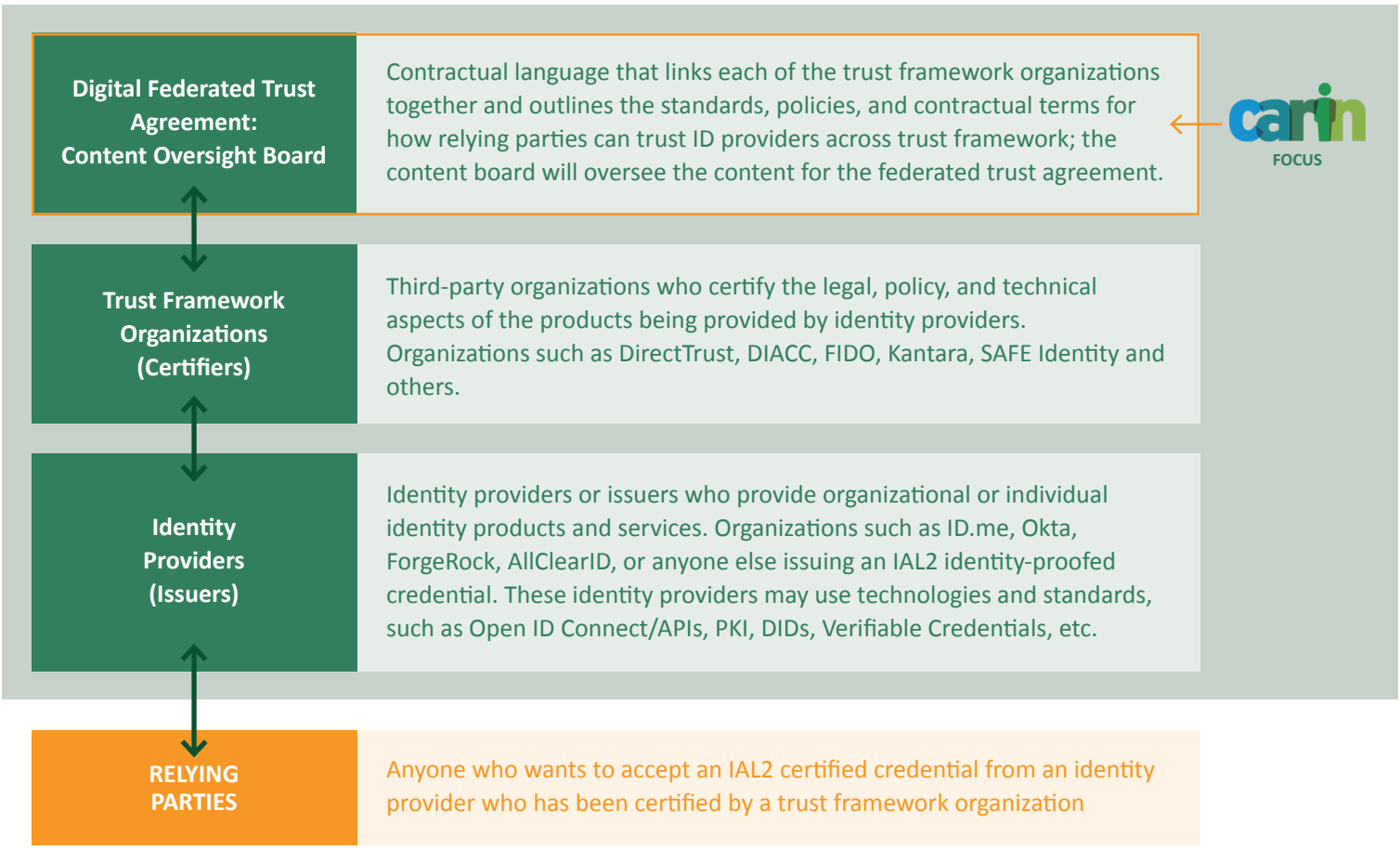
FEDERATED TRUST AGREEMENT: AN OVERVIEW

PURPOSE

Within a trusted federated digital identity ecosystem, there are identity providers or issuers which provide organizational or individual identity products and services. Trust framework organizations are third-party organizations who certify the legal, policy, and technical aspects of the products being provided by the identity providers. A relying party is any stakeholder which needs a trusted identity to exchange data. The CARIN Alliance seeks to develop a digital federated trust agreement which outlines the technical, policy, legal and certification guidelines necessary for equivalency to link each of the trust framework organizations together. The benefit of this approach is that a relying party, which needs a verified identity to authorize access to health data, can trust and rely on an identity credential provided by any identity provider who has been certified by a trust framework organization who participates in the federated trust agreement.

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 our paper addresses a specific approach for US health care, there could be multiple schemes and technologies associated with a specific trust framework.

TRUSTED FEDERATED IDENTITY ECOSYSTEM



SCOPE

In keeping with its purpose, the Federated Trust Agreement will include standards in each of the areas identified; new standards would be developed in areas where they do not already exist. Further, the Federated Trust Agreement would address conformity assessment, means of establishing assurance, and trust marking.

The scope of a trust framework and its associated artifacts is focused on policy conformance; this includes outlining the elements which would be assessed or measured in conformance testing to ensure that the Federated Trust Agreement requirements are being met. However, conformance testing itself and the methods would be outside the scope of the Federated Trust Agreement.

ASSURANCE

The Federated Trust Agreement assures that identity provider products and services, either as complete units or components, conform to a given standard or standards by trust frameworks. The outcome is a clear line of sight with accompanying liability from the consumer to the service provider, to the assessor, and to the governance board granting the trust mark.

FEDERATED TRUST AGREEMENT: OPPORTUNITIES TO IMPLEMENT

The Federated Trust Agreement can help advance the ability to exchange personal health information across systems electronically if it is implemented. We see a few potential pathways for implementing the governance structure associated with implementing the Federated Trust Agreement.

OPTION 1: INCLUDING THE FEDERATED TRUST AGREEMENT WITHIN THE TRUSTED EXCHANGE FRAMEWORK COMMON AGREEMENT (TEFCA)

A federal initiative known as the Trusted Exchange Framework (TEF) and Common Agreement (CA), known together as the TEFCA, will define the principles, terms, and conditions to "enable nationwide exchange of electronic health information (EHI)" while promoting high degrees of trust. The TEFCA seeks to establish a single onramp to participation in health information exchange for providers, hospitals, health plans, and other health care stakeholders, as required by the 21st Century Cures Act, so that EHI securely follows a patient so it is available when and where it is needed.[9]

The TEF guides the development of the Common Agreement. In Spring 2019, the Office of the National Coordinator (ONC) published an updated draft of the Trusted Exchange Framework (TEF), which outlines the set of principles that would promote trust and enable data exchange, and a draft of the minimum required terms and conditions to be included, along with additional terms and conditions voluntarily agreed to by the industry, in the Common Agreement.[10]

- The TEF principles in the most recent draft address key domains to provide guardrails for trust: (1) standardization, (2) transparency, (3) cooperation and non-discrimination, (4) privacy, security and safety, (5) access, and (6) population-level data exchange.
- The minimum required terms and conditions in the updated draft ensure common practices exist for entities which voluntarily agree to participate in the TEF. These include a common authentication process, a common set of rules for trusted exchange, and a minimum set of organizational and operational policies to facilitate EHI exchange.

The Common Agreement provides governance necessary to scale a functioning system built upon the foundation of the TEF. The main components are the Minimum Required Terms & Conditions defined in the TEF, Additional Required Terms and Conditions which describe the additional conditions required for day-to-day operation of a data sharing ecosystem, and a Qualified Health Information Network (QHIN) Technical Framework (QTF) which describes the technical specifications through which QHINs can accomplish the functional exchange requirements outlined in the Common Agreement.

[9]Office of the National Coordinator for Health Information Technology (ONC). (2019). Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2. Available at: https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf

[10]ONC, 2019

In the most recent draft of the TEFCA, ONC included a number of privacy and security requirements for information exchange in the Common Agreement, including that Common Agreement participants, regardless of whether they are Covered Entity or Business Associates as designated by HIPAA, need to promote the confidentiality, integrity, and availability of EHI by ensuring identification of individuals. The update clarified that the Common Agreement would adhere to Identity Assurance Level 2 (IAL2), Authentication Assurance Level 2 (AAL2), and Federation Assurance Level (FAL2) specified in the NIST SP 80-63-3 for federated models.[11]

The Sequoia Project as the Recognized Coordinating Entity

The TEFCA is administrated and implemented by a Recognized Coordinating Entity (RCE). In August of 2019, ONC selected The Sequoia Project to be the RCE.[12] As the RCE, the Sequoia Project has the responsibility of developing, implementing, and maintaining the Common Agreement in alignment with the TEF in partnership with ONC. This includes monitoring QHINs and modifying the QTF in the Common Agreement.

The Sequoia Project is a 501(c)(3) non-profit, public-private collaborative advancing implementation of secure, interoperable nationwide health data sharing. The organization plays a central role in convening public and private sector stakeholders to address interoperability; in 2012, The Sequoia Project took over management of the eHealth Exchange from the ONC and in 2014, The Sequoia Project, along with health IT leaders, launched the Carequality Initiative. Carequality is a network-to-network trust framework that connects existing data sharing networks and service platforms, allowing secure data exchange between networks such as vendor networks, payer networks, lab networks and others, such as the eHealth Exchange and CommonWell networks.[13] The Carequality Framework specifies the technical and policy requirements to enable data to flow between and among networks, platforms, and geographies. In 2018, Carequality was launched as an independent entity.[14]

Given Carequality's experience with the practical implementation of a health information exchange ecosystem that has many conceptual similarities to the QHIN exchange network to be enabled under the TEFCA, The Sequoia Project has engaged Carequality as a sub-recipient of its RCE cooperative agreement with ONC. Carequality's primary roles in the RCE work are to lead development of the QTF, and to implement operational processes around QHIN onboarding and ongoing monitoring and support. Carequality's existing specifications and requirements, while not always translating perfectly into the TEFCA paradigm, have informed work on the QTF, which borrows from the Carequality Framework where appropriate.

In 2020, the CARIN Alliance announced a partnership[15] with Carequality to advance interoperability and work together to improve consumer-directed exchange. Among the joint initiatives, Carequality and CARIN Alliance agreed to work on a common set of digital identity federation principles and accompanying operational elements to be implemented as contractually binding terms within the Carequality Framework. This would allow individual users to voluntarily create a person-centric digital identity credential and use that credential across all Carequality participants. As such, there is an opportunity to provide the Federated Trust Agreement to Carequality to be used in the Carequality Framework. This implementation within Carequality, in turn, can pave the way for the RCE to consider the Federated Trust Agreement for inclusion in the Common Agreement based on the timing, interest level, and specific requirements outlined by the RCE.

OPTION 2: INDEPENDENT NOT-FOR-PROFIT ENTITY

Another option is to establish a separate legal entity that is self-governed and managed according to a structured governance process. The governing body would be structured in such a way as to provide necessary compliance and continuity. Structures that could be considered include a 501(c)(3), 501(c)(4), or 501(c)(6) entity, which each confer their own advantages. This white paper will outline the governance and sustainability principles associated with setting up an independent entity that would be self-governed under one of these independent entity frameworks.

OPTION 3: INDEPENDENT WORKGROUP WITHIN AN EXISTING NOT-FOR-PROFIT

The federated digital trust agreement could also be managed and overseen using the set of principles listed below as a separate

[11]NIST, founded in 1901 and a part of the U.S. Department of Commerce, is one of the nation's oldest scientific laboratories. Within their purview they research and publish guidelines on identification and authentication for all entity types that need to establish confidence in their user and consumer communities. In 2013, NIST published a recommendation entitled "Electronic Authentication Guideline," most commonly known as NIST Special Publication 800-63-2. This guidance has matured over the years and version 800-63-3 was published in June 2017 and is the current specification to be applied in the U.S. for digital identity. It is from this source document that the foundation for identity proofing and authentication standards and regulations begins.

[12]Office of National Coordinator, 2019

[13]Learn more about The Sequoia Project at: https://sequoiaproject.org/about-us/

[14]The Sequoia Project (2020). What's the Difference Between eHealth Exchange, Carequality, and The Sequoia Project? Available at: https://sequoiaproject.org/about-us/whats-difference-ehealth-exchange-carequality-sequoia-project/

[15]Carequality. (2020). Carequality Blog: Consumer-directed Exchange. Available at: https://carequality.org/consumer-directed-exchange/

stand-alone workgroup within an existing not-for-profit entity. There are a number of existing not-for-profit health care entities that exist for the benefit of the entire health care ecosystem in which this workgroup could be established.

More conversations and input are needed with industry stakeholders to know which of the above organizational structures would be most appropriate. The CARIN alliance believes the principles outlined below associated with governance and sustainability are relevant regardless of which of the three possible organizational options listed above are chosen to implement the federated trust agreement.

FEDERATED TRUST AGREEMENT: GOVERNANCE AND SUSTAINABILITY

Regardless of which implementation path is selected, it's critical to the success of the digital federated agreement that an independent, balanced, sector-neutral governance body will guide and facilitate coordination between all parties involved in the digital identity ecosystem, including the identity providers that provide organizational or individual identity products and services; third-party trust frameworks organizations who certify the legal, policy, and technical aspects of the products being provided by identity providers; and relying parties, which use verified identity information to authorize access to data by relying on the Federated Trust Agreement. Additionally, it's assumed that such a governance body will be positioned to maintain and update the Federated Trust Agreement over time regardless of what organizational structure it lives in.

In this section, we outline a possible structure for the establishment of an independent, balanced, sector-neutral governance body and the functions it would be anticipated to perform to maintain the Federated Trust Agreement.[16] We are hopeful the proposal serves as a constructive starting point for further stakeholder dialogue. We urge all stakeholders to consider the proposed structure, engage in dialogue regarding ways in which it can be improved, and rapidly come to consensus as to a structure that can be broadly supported and established.

SCOPE OF GOVERNANCE

We believe the governance body should provide, through balanced, sector-neutral decision-making, trust across trust frameworks. Specific trust frameworks will certify the digital identity products and services provided by individual identity providers and will require their own governance activities within their own network or system which address specific systems and distinct standards and technologies they use (PKI, FIDO, API, DIDs, Verifiable Credentials, etc.). The Federated Trust Agreement is intended to sit a layer above, and be complementary to such activities by defining the standards, policies and terms so that relying parties can trust identity providers that use differing technologies and are certified across different trust frameworks. Ultimately, the development and evolution of identity products and services and the verification of those products and services by individual trust frameworks will evolve and should be encouraged, but governance is needed to ensure those distinct, independent identifies and their verification can be trusted across the ecosystem.

Therefore, the governance body described is intended to address the policy, process, and enforcement which impacts the integrity and reliability of trust across frameworks but is not specific to the technical substance of each identity approach or individual trust framework requirements. The scope of the governance body we propose herein is limited to the terms which allow relying parties to equally trust different identity providers and identity technologies certified by individual trust frameworks, and does not extend to governing the trust frameworks and identity providers themselves.

PURPOSE AND FUNCTIONS

The overarching purpose and function of the governance body described is to establish and maintain the Federated Trust Agreement to help advance the exchange of EHI electronically across the ecosystem.
To do so, the governance body is expected to:

1. Define the terms and conditions for the Federated Trust Agreement so that it meets its purpose, including defining policies, process and enforcing compliance among the members.

[16]The proposed governance and sustainability structure described is based on a White Paper published by the Pharmaceutical Distribution Security Alliance (PDSA), who is working to establish industry consensus on an interoperable way to track and trace prescription drugs in the pharmaceutical supply chain. PDSA is another alliance that is managed by Leavitt Partners, one of the co-authors of this white paper. The PDSA governance white paper is available for download at: https://pdsaonline.org/resource/pdsa-vision-for-phase-ii/

2. Assess the need for changes or updates to ensure the Federated Trust Agreement evolves as needed in the ecosystem and develops and manages the process so that it may be updated and refined.
3. Support the long-term sustainability of the Federated Trust Agreement.

Additional functions of the governance body may be identified as the governance body is developed.

Additional general operating functions will also be necessary to carry out those objectives and should be detailed in the governance body's bylaws.

GENERAL STRUCTURE

The proposed governance body is a membership-based organization with heavy reliance on committee activity and mechanisms for external engagement.

Leadership

Executive management of the governance body is the responsibility of a Board elected by the general membership. However, tactical work and other non-executive functions should be the responsibility of committees that are open to all general members.

Committee and Staff

Committees would be established by the Board, and participation in the committees would be open to all members. This is essential to ensure the broadest set of member representatives have input to the tactical work of the governing body. The Board will hire or contract staff to carry out the day-to-day management, but doing so should not undermine the importance of the committee structure.

External Engagement

Outside stakeholders (non-members) should also be able to engage with the governance body in three general ways:

1. The governance body should engage with appropriate federal officials and their delegates. For example, the Office of the National Coordinator (ONC) for Health Information Technology (IT) published the Trusted Exchange Framework and Common Agreement (TEFCA), which outlines a common set of principles, terms, and conditions to support the development of a Common Agreement (CA) that would help enable nationwide exchange of electronic health information (EHI) and named the Recognized Coordinate Entity (RCE). Similarly, the National Institute of Standards and Technology (NIST) defines federal digital identity guidelines in the four-volume special publication (SP) 800-63 Revision 3 (NIST 800-63-3). Their engagement with the governance body will provide valuable feedback on governance activities and should help the governance body be assured its activities and plans are consistent with expectations and needs in the field.
2. Committees may establish Advisory Groups composed of technical or process experts (e.g., thought leaders, standards bodies, service providers) to provide input on committee activities. These technical experts will be able to provide valuable insights and advice, and their participation in technical discussions should be encouraged.
3. Any interested stakeholder should be able to provide recommendations to the governance body, and the governance body should fairly and objectively consider those recommendations. It is recognized that outside stakeholders will have valuable ideas and recommendations for components of such a vision, and the governance body should welcome those ideas and recommendations.

MEMBERSHIP

There should be three classes of general members: (1) trust framework or third-party certifier members, (2) identity provider members, and (3) relying parties.

1. **Trust Framework or Third-Party Certifier membership** would be open to trust framework organizations or third-party certification organizations that (i) certify or define the legal, policy, and technical aspects of the products being provided by identity providers, (ii) attest to the Federated Trust Agreement, and (iii) agree to the representation, rules, and change process by the governing body.
2. **Identity Provider membership** would be open to any identity provider that (i) provides organizational or individual identity products and services (e.g. credentials) at an agreed level of assurance, and (ii) is certified by a participating trust framework member.

3. **Relying Party membership** would be open to any relying party that (i) accepts a certified credential from an Identity Provider Member who has been verified by a trust framework organization or certified by a third-party organization with membership, and (ii) accepts the Federated Trust Agreement. We believe the relying party constituency is the most important class of membership to ensuring federation works at scale in health care, and they will be prioritized as such within the governance structure.

Each member would, upon application for membership, designate itself as a specific member type. A member should be permitted to designate itself as a member of any sector in which it operates. The designated sector should not have to be the member's primary (e.g., highest revenue, highest volume) sector; it is a business decision for the member to determine the sector in which it would like its membership to be categorized. However, to prevent the gaming of voting structures by continually changing sectors, a member would be required to obtain approval from the governing body (specifically, by the Membership Committee, as discussed below) to change its designated sector.

The general membership would meet at regular and pre-defined intervals as appropriate. Additional meetings of the general membership may be called by a simple majority of the Board or upon petition by some proportion of the general membership.

General members would be accorded rights and responsibilities, including the right to participate in committees, elect board members, approve budgets, and ratify significant documents or changes. The membership structure and roles and responsibilities may need to evolve as the agreement and its governance evolve.

BOARD STRUCTURE

General Powers

The executive functions of the governance body would be the responsibility of a Board elected by the general membership. The Board would have the authority and responsibility to set the direction and strategy of the governance body. Additional responsibilities of the Board would include management of the board membership, financial decisions, committee management, and oversight over policies, procedures and technical specifications which significantly or fundamentally impact the Federated Trust Agreement.

Number and Qualifications

The structure of the Board is critical to provide appropriate balance among the various members. The CARIN Alliance is considering a mandatory rotation of seats, so every entity has an opportunity to participate on the board. There should be an odd number, 5-17 is usual, of Board members to achieve this balance allocated as follows:

1. A set number of Board seats would be open to, and elected by, general members who are **trust framework or third-party certifier organizations**. These seats are referred to as trust framework or third-party certifier board members.
2. A set number of Board seats would be open to, and elected by, general members who are identity providers. These seats are referred to as **identity provider board members**.
3. A set number of Board seats would be open to, and elected by, general members who are relying parties. These seats are referred to as **relying party board members**.
4. The remaining Board seats would be considered **at-large board members**. These seats would be open to any general member regardless of type, provided that at-large seats may not be held by members from the same sector. Unlike the other Board seats (which are elected by a vote of only the members from the respective sector) all members would vote for at-large candidates.

Any general member would be eligible to run for its type's Board seats or an at-large seat; provided, however, that a single organization, either directly or through its corporate businesses, could not control more than one board seat at any given time.

Term of Office

Board members would serve staggered 3-year terms. Therefore, a portion of each sector's seats would be open for election each year, and a portion at-large seat will be open for election each year.
Terms limits would not be imposed, recognizing that Board members would have to stand for election every 3 years.

The benefits of staggering terms include maintaining continuity between terms, preserving historical knowledge, and reducing the overturn of changes or updates made by previous governance leadership.

Nomination and Election
Accountability to the general membership via the annual election process is also a critical attribute of the Board.

Board nominees would be self-nominated or nominated by a peer and would be elected by simple ballot with the top vote-getter obtaining the seat. Any ties in voting for Board members would be broken by a vote of the remainder of the Board whose seats are not standing for election in that cycle. If there are no nominees for a seat, the members from the respective type(s) would recommend a representative from the relevant sector to fill the seat. The Board would approve that recommended replacement if he or she meets basic criteria to serve.

Each Board seat would be held by an individual in his or her capacity as a sponsored representative of a specific member type. As a result, if the individual elected to a Board seat leaves his or her organization – or is otherwise unable to serve – the individual would not retain the seat. Instead, the member organization will recommend a replacement for approval by the remainder of the Board. The Board would approve that recommended replacement if he or she meets basic criteria to serve. If such replacement cannot be identified, the Board would select a replacement (from any member organization in the sector) to serve for the remainder of the term. Regardless, each Board member has a responsibility to act in the best interest of the governance body.

COMMITTEE STRUCTURES

Committees would be used to carry out most substantive and tactical work of the governance body. Five initial committees will be established upon formation of the governance body: A Membership Committee, a Finance Committee, a Policy Committee, a Standards Committee, and a Conformance and Certification Oversight Committee. The Board would be responsible for appointing a chair of each committee, but participation in each committee to would open to all general members.

The **Membership Committee** would be responsible for the development, recruitment, and retention of membership.

The **Finance Committee** would be responsible for financial planning for the governance body, including the development of an annual budget for Board consideration and approval.

The **Policy and Standards Committee** would be responsible for substantive, tactical, standards, and policy work related to Federated Trust Agreement.

The **Conformance and Certification Oversight Committee** would be responsible for engaging with, supporting, and advising the Board and Policy Committees all facets of compliance monitoring and certification related to Federated Trust Agreement.

The Board would be responsible for establishing the general direction and strategy of the governance body, including coordination among the committees. Committee chairs would have significant latitude, however, to operate within the general framework set by the Board, including the authority to set and manage the agenda and work plan for each committee. All committee activity would be conducted by simple majority of committee members, unless otherwise necessary.

OTHER PROCEDURAL SAFEGUARDS

As the specific activities of the governance body are further defined, additional or alternative procedural safeguards may be needed to ensure legal compliance. Stakeholders who come together to form the governance body should be diligent in their review of the final structure on which they agree to ensure compliance. For example, if the governance body will engage in standards setting activities, it will be essential that appropriate procedural safeguards are in place to ensure openness, balance, due process, appeals processes, and consensus development. Additionally, the governance body should immediately develop and adopt appropriate policies and procedures, such as policies for identifying and assessing potential conflicts of interest.

FUNDING MODEL

The ultimate funding model for the governance body should sustain the governance body functions and be determined by the founding members. Members approve the funding model, and any potential dues annually in accordance with their rights and responsibilities.

CONCLUSION AND NEXT STEPS

The CARIN Alliance envisions an ecosystem where an individual voluntarily creates a single, identity-proofed digital identity credential for use in an application of their choice which they own, manage, control and use to access their health information from any health care payer or provider in the country. To facilitate this ecosystem, the CARIN Alliance is in the process of developing a federated digital trust agreement which outlines the technical, policy, legal and certification guidelines necessary so digital credentials can be trusted even when they are issued and certified by differing organizations and agnostic to their underlying technology. We believe this which will advance the ability to exchange personal health information across systems electronically.

Our call to action for the industry is simple:

Step One
Implement the **SMART Application Launch Framework** that is required under the ONC and CMS rules today which allows an individual to access their health information today from an application of their choice using their portal user name and password,

Step Two
Engage an identity provider (IdP) that can create or receive a NIST 800-63-3 identity assurance level 2 (IAL2) digital credential that includes support for strong authentication credentials which meets the requirements of an authenticator assurance level 2 (AAL2) or higher and then ensure the IdP meets the appropriate conformance requirements of one on the trust framework organizations listed in our whitepaper, and

Step Three
Engage with us and the OpenID Connect Foundation in 2021 to participate in identity federation pilots with multiple relying parties so we can develop an approach as an industry and as individuals for how an identity federation approach could work in health care that allows for an individual to be in control over their own personal identity credentials across systems.

BACKGROUND ON THE CARIN ALLIANCE

The CARIN Alliance[17] (CARIN) is a bipartisan, multi-sector collaborative working to advance consumer-directed exchange of health information. CARIN's vision is 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. An essential component to achieve meaningful consumer-directed exchange is the ability to identify individuals correctly digitally across systems and is a focus area of the CARIN Alliance. For more information, please visit **www.carinalliance.com**.

[17]For more information, please visit **www.carinalliance.com**

We want to thank the following organizations who participated in the drafting of this white paper:

Organizations who participated and may sign the Digital Federated Trust Agreement

Carequality
DirectTrust
The FIDO Alliance
Kantara Initiative
SAFE Identity

Other supportive individuals and organizations who participated

ID.me
1up Health
Cambia Health Solutions
Ciitizen
CVS Health
Dev Dash, MD, MPH, Stanford Health
EMR Direct
Mastercard
OpenID Foundation
PRIVO
Videntity

APPENDIX – THE DIGITAL FEDERATED TRUST AGREEMENT: TABLE OF CONTENTS

Attached below is a draft table of contents for the digital federated trust agreement that would be signed by each of the trust framework organizations who are participating to ensure equivalency of conformance testing when identity providers use any of these trust framework organizations to execute their policy and technical conformance testing. Each of the trust framework organizations are working collaboratively with the CARIN Alliance to finalize a draft of the digital trust agreement. Our current timeline is to publish an initial draft for industry review in 2021.

I. Definitions and Terminology
- a. Standards referenced
- b. Glossary of terms

II. General Terms and Conditions
- a. Other business and legal matters

III. Governance and Accountability
- a. Policy, Rule, and Requirements Development
- b. Certification, Accreditation, Assessment, and Audit
- c. Infrastructure (Technology and Operations) Assessment
- d. Policy Administration
- e. Publication and Repository responsibilities
- f. Compliance Audit and other assessment
- g. (As required) Certificate Usage
- h. (As required) Prohibited Certificate Use
- i. (As required) Certificate Policy
- j. (As required) PKI entities

IV. Interoperability
- a. Standards Development
- b. Specification Developments and Exchange

V. Administration and Operations (Issuer)
- a. Redress and Recovery
- b. Enterprise Governance
- c. Internal Audit
- d. Service Optimization
- e. Updates
- f. Facility Management and Operations/Technical Security Controls

VI. Functional (End User)
- a. Registration
- b. Credentialing
  - i. Credential Issuance
  - ii. Credential Suspension
  - iii. Credential Recovery
  - iv. Credential Maintenance
  - v. Credential Revocation
- c. Notice and Consent
- d. Privacy
- e. Verified Person
- f. Verified Organization
- g. Relevant aspects of the Minor's Trust Framework[18]
  - i. The Minor's Trust Framework is an approach to fostering the adoption of online identity trust services that focuses specifically on children's identity and parental consent within the context of complying with the Children's Online Privacy Protection Act (COPPA) and emerging international policies.
- h. Authentication
  - i. Authenticated Session Initiation
- i. (As needed) Certificate Life Cycle

VII. Independent Certifiers
- a. Criteria for selection

[18] https://www.privo.com/mtf-laws-and-regulations and https://www.oixnet.org/registry/minors-trust-framework/