FIRE and HIA WG’s, members are in their 5th version of a working draft in providing content for a new Kantara Charter. There’s agreement on the internet’s explosive enterprise of connected things, i.e. smartphones, applications, networks, identifiers, API’s, and sensors, and the impact on privacy, security, access controls and the need for trusted digital identities. We have, in past workgroup activates, recognized there are a number of preconditions and assumptions that have to and will be made as part of a fundable action plan.

In an article from McLean Research, Harvard Medical School Affiliate, referencing **Pew Research Center, 69% of adults and 81% of teens in the U.S. use social medial.** This is a large amount of the population that is at risk for depression, anxiety or other chronic and medical issues due to poor habits relating to both on-line and off-line determinant lifestyles. Even when they feel ill they’re back on-line. Hard to define a positive outcome when there’s not a trustworthy place to support a change in behavior.

The article defined this time as the **Digital Age of Vulnerability** with the three leading social medial sites nationally making little effort to make a positive change.

On a positive note, HHS’s Office of Inspector General issued (last month) an opinion supporting incentives, with compliance guidelines, relating to behavioral and substance issues with each patient having a unique set of goals established by their provider. The program recognizes the value in using a smartphone. It is important to note that collaborative evidence is required as part of the process including a digital identity

So now the real work begins: we need to answer the following questions when engaging the internet:\*

* The FIRE and HIA WGs are working from the legacy Identity Ecosystem Framework (IDEF): What is a Trusted Identity? What is a Framework?
* What does an individual, granularly, want to feel? Trust!
* How might a trust attribute be cultivated? Most likely where they are?
* What is the social and support system profile of their community?
* We have experienced face-to-face trust: How do you know

who I claim to be? What assurance do you have it’s me?

* Yes, I have a smartphone, you say it does what? How

can I trust that ‘device’ with my confidential info or private data?

* How do I trust the person speaking that I don’t know? Have not heard of that company, how can you trust them? That application, how do I trust it with my data and who has access to it?
* How does a user gain a ‘comfort level of trust’ when online?
* Would an incentive (a beneficial value) from a local vendor spark interest?
* Is there a possibility to create economic mobility on behalf of that user?
* Does such create a health equity value for a user that can be measured?
* For a user this could be as a place-based, living experience for building trust?
* \*This document is a high level outline and if accepted by the WG’s it is understood that we will have to generate similar specification document that were submitted to ONC last year, not part of the charter effort but a first year achievable goal.

Participating work group (WG) members collectively underscored the need to develop a consumer-centric strategy to help individual, online users gain insight on what a Trusted Identity is and the value and risk protections it could bring an online user. Our WG would need to outline and define basic steps on how one might develop online trust, as well as trust in their own mobile devices, then test examples with feedback from different age groups, cultures, markets and industries. As noted in earlier discussions, a consumer’s authenticated, trusted identity must be portable and adaptable to sectors/industries of their choosing. Since healthcare is highly regulated, representing a fifth of the nation’s expenses annually, integrates with multiple industries, and in requires a trusted identity solution, it is the WG’s recommendation and complements Kantara’s mission.

Target Market Sector: **Vulnerable Patient Populations**

Patients with chronic conditions, disabilities or low income represent significant economic and societal costs in terms of disability payments, bankruptcies, and lost productivity. If a trusted identity solution is adopted by Government, savings could be a beneficial windfall so incentives should be a consideration with supporting audit trails. In healthcare there is a very positive upside for patients and payers when patients are compliant in taking meds, following care plans, and managing chronic conditions.

**Populations to Consider**

**Chronically ill and disabled\* Patient profile – 15% to 20% of this population**

**Medicare-seniors; Medicaid-low income families – Payer-grouping**

People with chronic diseases are at risk of poor health outcomes, they consume more healthcare dollars than healthy individuals. The chronically ill are twice as likely to report poor health days as the general population. Disabled individuals have many interactions with the health system, but, due to their disability, they may have difficulty accessing care.

**Low-income and/or homeless individuals\* Patient profile – near 20% of population**

**Medicaid, Public Health low income families – Payer-grouping**

In general, low-income individuals are more likely to have chronic illnesses, and the impact of those illnesses can be more severe. People with low incomes are also disproportionately racial and ethnic minorities. Being low-income, they may be less likely to have coverage and, as a result, have less interaction with the healthcare system**.**

**\***The majority of both population sectors have access to and use smartphones, many using social media platforms. According to the American Journal of Managed Care, Behavioral Health issues escalating in all age groups (including children) and more seniors are adopting smartphones and connected technologies, but privacy and security are high-level concerns. Integrated technologies and secure data sharing for government-supported programs will be triangulated between medical providers, payers and patients and their delegated representative.

During the 2020, Covid-19 crises, the **public health population** across the country was seriously impacted due to lack of documented core social determinants in government health records, (Venerable Populations: Developing and Sustaining Community–University Research Partnerships: To Reflect on Relationship Building Jan 1 2022)relating to personal poverty, food security, housing stability, living conditions, and lack of access to transportation. Yes, health service and food stamps were provided but data was siloed in separate public health and welfare systems and not always accurate or was missing. Last year (2021) the Healthy People 2030 Trusted Source campaign was launched. Government also recognizes conditions in the environments, or Social Determinants of Health (SDOH), where people are born, live, learn, work, play, worship, and age significantly influence their health. The 2030 goal is to have valid, reliable, nationally representative identified data.

\*Noted above, the majority of individuals in this healthcare sector population have smart phones with social identities and they will be future candidates with the support of local governments and local social service entities. With the [Executive Order for Zero Trust](about:blank) by late 2024, NIST’s response to the Executive Order with the draft [Recommendations on Criteria for Cybersecurity Labeling for Consumer Software and Internet of Things-Products](about:blank), is setting the stage for a ‘Trusted Identity’ process at some assurance level at State and local government levels. The individual, being an online user, most likely will seek some valued content support from a trusted, not-for-profit source like Kantara.

Future subject material for Trusted Identity discussion relating to VPs:

* Relying Parties
* Access Controls
* Identity Assurance Level
* Authenticator Assurance Level
* Federated Infrastructure and Identities
* Internet of Things/Smart Medical Devices (CMS-FDA)

[https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf](about:blank)

[https://link.springer.com/referenceworkentry/10.1007/978-3-030-58675-1\_58-2](about:blank)

steak

digital ledger Distributed

https://kantarainitiative.org/confluence/display/archive/Report+from+the+Blockchain+and+Shttps://kantarainitiative.org/confluence/display/archive/Report+from+the+Blockchain+and+Smart+Contracts+Discussion+Group

https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=144016373mart+Contracts+Discussion+Group