RECAP
CARIN Health Care Digital ID Summit
June 4, 2019 | Washington, D.C.

Representative Attendee Organizations

All Clear ID, American Association of Retired Persons (AARP), American Association of Motor Vehicle Administrators (AAMVA), b.Well Connected Health, Blue Cross Blue Shield Association (BCBSA), Boston Children's Hospital, Cambia Health Solutions, Capitol One, The Center for Medicare and Medicaid Services (CMS), Cerner, Coral Health, Direct Trust, Dr. First, EMR Direct, Epic, Humana, ID.me, IPRD/Gates Foundation, Kaiser Permanente, Kantara Initiative, Lush Group, My PatientLinks, New Jersey Health Information Exchange, Northwestern University, The Office of National Coordinator (ONC), The Pew Foundation, Regenstrief, Sage BioNetworks, Sequoia Project, Singular Key, Inc., United States Digital Service, Venable, VISA

Objectives and Format

- CARIN Health Care Digital ID Summit participants gathered to discuss the four specific questions associated with the use of application programming interfaces (APIs) built with Fast Healthcare Interoperability Resources (FHIR) to share both clinical and claims data with consumers, third-party applications, and others within the health care ecosystem:
    1. How do we identify unique users across systems using person-centric mobile technologies?
    2. How do we securely authenticate individuals across systems using modern, open standards?
    3. Once a patient is identified at one organization, how do we cross-facility match a patient to their records?
    4. What does a consumer-directed, electronic federated consent approach look like?
- There were 10 'toolbox' presentations that addressed potential solutions to the five problems surfaced: (1) identity, (2) authentication, (3) trust & federation, (4) consent, and (5) matching. See companion document for copies of the presentations.
- Breakout workgroups gathered and discussed each of these problems in detail. Specifically, groups considered best practices and standards in each area, how government can support implementation, and a list of remaining open questions. The workgroup summaries are below.

Breakout Sessions

1. IDENTITY

- Use Case Question: How should remote ID proofing events occur via applications and what organizations should be involved in the ID proofing event?
- *Best practices and open standards recommended for industry adoption in the next 2-5 years:*
    - Standards for identity exist; **NIST 800-63-3 is the preferred choice** because it is the most germane and provides guidelines for the identity proofing process (IAL2 is the preferred level in health care), and digital authentication process (AAL2 is the preferred level in health care). Use of these standards can mitigate some of the vulnerabilities inherent to digital information exchange when privacy needs to be protected.
    - The shift from a traditional Fee-for-service (FFS) payment approach to more managed care (MC) escalates the need to identify and access longitudinal patient data. Providers also have an incentive to engaging in identity proofing because it can improve claims matching and billing. This creates an incentive to solve the identity problem, and to cooperate in the industry.
    - Ultimately, there needs to be standardized data element profiles that can be transmitted or shared in a consistent manner. The goal is for an ID proofing event to

happen using PII attributes (e.g. biometrics) and for that event to happen as infrequently as possible to minimize consumer friction (reuse is possible).

- *How the government can incentivize implementation:*
  - While the government's ability (specifically the Government Services Administration) to drive this work forward is unknown, GSA could include stronger language in legislation to put an assessment process for NIST 800-63-3 in place. This would include documented standards for digital credentials (e.g. establish that an organization which establishes identity and issues credentials is a 'good actor.').
    - The group noted that GSA FICAM Trust Framework Solutions (TFS) did authorize and contract Trust Framework Providers at the time of 800-63-2 to undertake assessments, approval and trust marking of compliant solution service providers. Some of those contracts are still in force today.
  - Instituting uniform federal compliance with NIST 800-63-3 would be beneficial. For example, the DEA regulation points to NIST 800-63-1 and in the future could point to NIST 800-63-3.
  - There was discussion about an assessment process and which agency could offer these services – GSA, FICAM, TFS came up; CMS's creation of CCHIT was also referenced as a model that could be used for identity proofers.
- *Outstanding questions and concerns; other comments:*
  - Who are the other non-governmental groups - besides those who were present at the summit - that can drive work forward on identity and what are their roles?
  - Is there a process that doesn't include IAL2? For instance, FIDO2 doesn't need it and a global standard process already exists.
  - While NIST 800-63-2 included a provision or process for assessment and allowed entities to become certified assessors, NIST 800-63-3 does not. This is a significant gap.
  - There are inherent patient challenges concerning identity – e.g. homelessness or not having a valid form of identification.
  - There are existing entities who can provide identity verification – e.g. AAMVA (Driver's License Validation), State Department/Department of Homeland Security (Passport Validation), or the Social Security Administration.
  - The Trusted Exchange Framework and Common Agreement (TEFCA) could have a dramatic impact on the identity landscape since it requires IAL2 and AAL2. Will there be penalties for failing to comply with TEFCA? What role could the RCE play in helping to implement IAL2?

2. AUTHENTICATION

- *Use Case Question:* How can the provider or other data holder through an application know that the patient is the one making the request at that moment?
- *Best practices and open standards recommended for industry adoption in the next 2-5 years:*
  - The group discussed FIDO (specifically FIDO2), as a type of two-factor authentication, its capabilities and limitations at length. **Group agreed FIDO is an effective open standard that could be used in health care.** FIDO is being used extensively outside of health care and will eventually be ubiquitous on billions of mobile and desktop iOS and Android devices over the next 12 months.
  - The group discussed promising solutions for universal two-factor authentication which are currently proprietary. This includes behavior biometrics and risk-based interactions. These are being standardized from the design side in mobile operating systems but are

largely proprietary from the risk/security side (e.g., know your customer processes at online banks and trading platforms).
    - The group agreed health care needs to adopt open standards. Proprietary versions of standards are not scalable across multiple sectors of the industry.
- *How the government can incentivize implementation:*
    - The recent OMB memo allows for authentication flexibility at the agency level if the standards of IAL2 are met. This is good – it will signal to the market and catalyze innovation. However. it was noted that this applies only to federal agencies.
    - ONC could choose to join the FIDO Alliance, which provides open source specifications and standards, or point to FIDO as part of future regulatory activity. Ultimately, policy will drive change.
    - The group highlighted the variability across government programs and expressed concern it was arbitrary and should be resolved. For example, the DEA regulations are very prescriptive and outdated. New technologies resolve their previous concerns (e.g. it is possible to protect authentication processes in a single device from each other), and regulations should be updated and uniform. Also, the group noted that TEFCA rules are voluntary and likely not going to drive innovation as currently written.
    - The government may be able to help the industry by sponsoring projects that would pair biometrics on a device and the people interacting with the device.
- *Outstanding questions and concerns; other comments:*
    - Risk splitting is an outstanding concern – it is possible to flag if something is abnormal but largely unable to resolve.
    - The group considered whether government guidance would drive change.
    - The group noted that FIDO2 relies on on-device biometrics and there was hesitancy to move biometric data off device. A centralized biometric database is a serious privacy and security concern.
    - Another concern with FIDO2 is that if you lose the device, you lose the token and would need to reauthenticate on your new device.
    - While FIDO adoption is not yet ubiquitous, FIDO is a good authentication solution because it allows for flexibility and can be used on multiple device types.
    - Another critical aspect in this area is measurement. The industry may be required to implement IAL2 but there needs to be measurement in order to issue guidance on it. Standards for measurement and certification need to be developed and used.
    - The FIDO Alliance is currently working on a number of issues: tying identity proofing to authentication, addressing 'man in the middle attacks,' and others. Representatives invite stakeholders to join the FIDO Alliance and test their use cases.

3. TRUST AND FEDERATION

- *Use Case Question:* How can the receiver leverage the ID proofing event that has already occurred through an app and previous provider or data holder?
- *Best practices and open standards recommended for industry adoption in the next 2-5 years:*
    - We need best practices to ensure that there is a strong identity linked to a strong authenticator; having a weak identity or weak authenticator renders the information useless.
    - A digital signature standard to convey trustworthiness should exist.
    - Baseline rules should be established to dictate how participants will act across communities; however, it shouldn't be overly prescriptive. The group advocated for a reasonable floor, or baseline behaviors which should be observed across players.

- Group agreed on a few key ideas related to a trust federation ecosystem: There should be an operating agreement, language uniformity, HITRUST certification (where appropriate), federated trusted credentials from third parties like CARIN Alliance and others, and dynamic registration of applications.

- *How the government can incentivize implementation:*
  - The government can provide incentives and remove disincentives. This is particularly relevant because some areas are subject to network effects and will need a 'jump start' to overcome barriers to entry.
  - The government can also issue guidance, implement regulation, and provide oversight/ verification to ensure that everyone is treated fairly and acts in good faith. However, the group is sensitive to what is too much regulation and too much oversight. There is resistance in part because federated login evolved without a government mandate. The cost to participate could be prohibitive for some companies. Group did not want to discourage new entrants or start-ups and want to promote a flexible network of providers and users.
  - There was discussion there may be a need for federal enforcement of penalties for bad actors. Workgroup members suggested including regular auditing and voluntary oversight and enforcement.
  - The government can lead by example as it has done with the Blue Button 2.0 initiative and it can be an open identity provider (e.g., healthcare.gov, login.gov, etc.).
  - There is an opportunity for the government to host demonstrations or sponsor pilots to jump-start progress.
  - Safe harbors could limit apprehension when organizations rely on identity and authentication events that originated with other parties. This would effectively limit the liability if an entity acting in good faith trusted another identity which made a mistake. Examples of safe harbors included allowing a duplicate identity if the provider doesn't trust the other system and purchasing liability insurance.
- *Outstanding questions and concerns; other comments:*
  - There is overlap across the five topics discussed; the group noted points about device-to-owner authentication and system-to-system authentication are issues of trust.
  - Health care is unique because it is the only industry where there is proposed federal regulations that would require data holders to share information with the patient and allow the patient to choose any application of their choice.
  - Technically, there are existing ways to express identity, authentication and trustworthiness (OpenID, UDAP, etc.), but there is a need to extend them further. They are still fairly silo-ed because they are used to solve existing issues rather than supporting federation.
  - There is an opportunity to learn from other sectors (e.g. UK banking or the anti-fraud banking group).
  - There is still some question about whether the industry will accept the reuse of credentials or if they will ever accept identities they don't control.

4. CONSENT

- *Use Case Question:* How can the sending and receiving third-party applications know that the patient has consented to how she wants her health information used by the application?
- *Best practices and open standards recommended for industry adoption in the next 2-5 years:*

- In the best-case scenario, people would understand what they are releasing, from and to whom, for how long, whether they have the right of revocation, and what the risks of that consent are.
- There should be guidance and standards for consent and the elements included to ensure informed consent.
- Consent should live in a centralized database or be federated from individual devices.
- It should be standard for the consent permission to travel with the data (meta-data element), and the app should have technical capability to convey that consent has been completed to a receiver.
- Currently, no floor exists for consent but there should be. It is attractive to create a floor but where it should be is difficult to identify.

▪ *How the government can incentivize implementation:*
- Federal government can give guidance on informed consent.
- There are extra-governmental mechanisms too:
  - CARIN Alliance could create standards and example templates for consent that meet those standards for open adoption. Health care organizations can support adoption by refusing to release data without receiver demonstrating that the standards are met.
  - CARIN could develop standards and example templates which are trademarked. This would create an enforcement mechanism and may drive greater adoption. Model standards included Kantara's consent receipt and the university IRB process. ISO is also working on a consent receipt standard.
- Independent of who develops guidance, the developer should include templates to seed good practice for open use. The easiest path should be the path that does the right thing.

▪ *Outstanding questions and concerns; other comments:*
- There should be special consideration given to consent given the general literacy and health literacy levels of the US population.
- There was discussion about whether levels of consent could be used. In such case, less consent would be required for aggregate queries, but higher levels of disclosure and storage may require more consent.
- The group discussed whether there could be a 'white list' of apps or app developers who follow basic consent best practices including the CARIN code of conduct. HC organizations and providers can choose more wisely using this list.
- There was a question of whether consent could be provided as a service and participants believed that there are private companies which offer consent authorization.
- Concerns about weaponized third-party apps and individuals versus communitarian consent were expressed.
- Sage Bionetworks resources are open source and can be implemented. These are open source because there was a desire to not want to be prescriptive or 'force the hand of an organization.'
- There was concern about sharing consent information because consent itself is PHI.
- Generally, there was the belief that much progress needs to be made in order to federate consent.

5. MATCHING

▪ *Use Case Question:* How can the receiving provider know they are connecting the health records of the right patient?

- *Best practices and open standards recommended for industry adoption in the next 2-5 years:*
  - The group believe there is an intersection between OpenID Connect and FHIR which can help move patient matching forward.
  - They focused on recommendations which fit the prescribed timeline:
    - **There should be a standardized and agreed upon data set for matching. This should include, at a minimum, USCDI combination and additional elements (e.g. insurance policy number, email address, and historical information - like addresses.).** There was some conversation about creating standards for individual data elements, but it is probably only necessary for certain elements.
    - **Group agreed adopting an IAL2 certified credential would go a long way to solving the patient matching issue.**
    - Incentives need to be in place so that the data elements are captured. Data capture could occur at point of care (e.g. payer, provider), through an HIE, on phone/ device or through some combination. The group suggested incentives could be negative or positive.
    - Demographic data is useful for patient matching, but more advanced data elements should be examined and incorporated. This surfaces technical and privacy concerns but should include device or biometric elements. Works needs to be done to incorporate these data elements into the infrastructure.
    - Health care is behind every other industry in this capacity and instead of recreating the wheel, we need to coordinate, collaborate, and adopt the approaches that are already in use. FHIR is an example.
- *How the government can incentivize implementation:*
  - Participants believe the governmental will be instrumental in pushing this work forward because health care organizations will be slow to adopt or address unless they are required to.
  - The government can prescribe standards and mandate data collection through its payment authority. For example, CMS could mandate that required data elements are collected by payers.
- *Outstanding questions and concerns; other comments:*
  - There was some disagreement on whether to use FHIR or ConnectID. Some participants wanted to embed ConnectID in FHIR.
  - Participants underscored the importance of leveraging existing matching approaches. The group agreed that it is incumbent on the them, as leaders in the field, to connect and partner with others working on matching and other issues of identification.
  - Others noted that healthcare is still unique from other sectors; this includes concerns with and accounting for minors, twins, and caregiver authorization.
  - There was some discussion about how matching and identity proofing at the point of care and how it could mitigate a tremendous amount of patient matching expense.
  - Some participants believed there was a clear and distinct delineation between identity proofing and matching whereas others felt that they are inextricably linked.
  - There is no market for linking healthcare providers to the identity standards community.

Next Steps

- Develop action plan and investigate proof of concept opportunities
- Further explore funding for a pilot through federal and private means
- IDentiverse in June 2019 & Health 2.0 in September 2019 are chances to share this group's thinking