CARIN Technology Workgroup Meeting
Authentication and User Proofing Discussion

October 30, 2017 | Washington, DC

Objectives

Members of the CARIN Alliance met with a goal to begin work on developing the requirements and a technical approach for how a consumer can remotely user proof and authenticate themselves via a mobile device/app and access their health information from multiple sources.

- Major Questions:
  - Can we **user proof** individuals outside of the provider portal using a federated identity structure and existing or evolving open standards without the need for a centralized, commercial third-party database?
  - Can we securely **authenticate** individuals using 2-factor authentication without the need for a UN/PW?
  - Can we record electronic **informed patient consent** in a consistent way to facilitate the delivery of patient health information to a third-party application of the patient's choosing?
  - Can we **record match** a patient's existing medical record information using KBV/KBA questions from the EHR using installed FHIR resources?

Key Discussion

User Proofing

- The group reviewed the NIST IAL/AAL matrix
  - Authentication is getting easier, but identify proofing is getting harder
- Use Case for ID Proofing
  - The group considered the importance of having a "traffic cop" to ensure the ID proofing event is done correctly and is trusted
  - Open questions exist around whether this would be ID Proofing or federated access under FICAM standards
- Vectors of trust is an emerging open standard to help communicate what level of user proofing and authentication has been done by another party
  - This communicates trust, but does not establish trust between parties who are involved
- Future work needs to focus on operating rules and the potential role of a registration authority

Authentication

- There are three things needed for federated identity to work:
  - Trust framework
  - Utility for user proofing/authentication
  - Linkage to social media or other accounts
- FIDO Standards is a well-used emerging open standard to authenticate individuals using their mobile device, biometrics, and cryptography.
  - Currently, FIDO is used by Aetna, Amazon, AMEX, Google, Microsoft, Samsung, VISA, Motorola, many of the largest financial institutions in the world, and more.
  - The FIDO specification can be found here.

Informed Patient Consent

- Group agreed patient consent (or the individual right of access) is assumed once the patient has user proofed themselves and authenticated with a covered entity. CMS also indicated they are configuring a 'set it and forget it' period of time (5 years) for Medicare Blue Button with regular notifications on what apps are connected.
- Creating ways to make sure a patient is truly informed about the consent they are giving will be key
  - How can the group work to make the information consumers are receiving easy to understand?
  - There are open questions on what information can be shared
    - The consensus of the group was it's extremely difficult for consumers to select which fields in the CCDS should be sent to the third-party application. As of now, the group recommended an "all or nothing" choice to send the data given the complexities of parsing it outside the EHR
- The AHIMA form for individual access may not be an effective path forward when we move to paperless access since it's focused on the entire medical record and relies more on copying rather than sharing information.
  - Using a third-party application will help streamline the electronic individual right of access request

Record Matching

- Knowledge based verification and knowledge based authentication can help with record matching
- Group discussed exploring ways for the consumer to create their own identifier when the data is pulled

Next Steps

- Build out a series of use cases as part of the trust framework that matches the appropriate AAL/UAL levels in the NIST matrix for providers and vendors to follow. Leverage the work being done in the private sector and as part of the Heart workgroup.
  Responsible Parties: Catherine, Debbie, and LP will take the lead

- Alliance for Better Health (NY DSRIP) will take the lead in building out a technology utility that can be used to ID proof individuals for specific use cases that include SDOH
  Responsible Parties: The **Alliance for Better Health** will develop an RFP to begin the build out with the hope of standing something up by Q1 2018. The **CARIN Alliance** will provide requirements support and a technology lab in which to 'test' the utility

- Develop the technical approach for linking a consumer's social media log-in to the patient portal registration process
  Responsible Parties: EHRA, Argonaut (Micky), CARIN Technology WG

- Further explore the ability to leverage the FIDO 2-factor authentication standard in health care
  Responsible Parties: EHRA, Argonaut (Micky), CARIN Technology WG

- Begin exploring electronic individual right of access requests in the market today (i.e., NIH's All of Us program, MI HIE, etc.) to examine ways to present a uniform and understandable way for the consumer to understand what they are consenting to and the risks involved
  Responsible Parties: CARIN Trust Framework – Consumer Engagement workgroup

- Begin exploring how to create an ecosystem of trusted third-party applications (i.e., Xcertia)
  Responsible Parties: CARIN Technology Workgroup

- Consider the open banking work being done in Europe related to ID proofing, authentication, and consent
  Responsible Parties: LP to review with NIST and Jeremy