The CARIN Alliance
[Creating Access to Real-time Information Now through Consumer-Mediated Exchange]

CARIN Trust Framework Forum
December 8, 2016 **|** Washington, D.C.

Objectives

- Set a shared context regarding the new world of consumer-directed exchange (CDEx) of health information
  - o Identify the need for a trust framework
  - o Begin to shift the mindset from the old world of optional data sharing to the new world of mandatory data sharing
- Determine priority use cases for the CDEx Trust Framework
- Identify top trust-related barriers to CDEx
- Discuss key open questions for CDEx
- Determine a path forward to addressing gaps and developing a trust framework

Setting the Stage

- CARIN was formed in May of 2016 with a vision to have a united health record that moves with consumers/patients when, where, and how they want it to help improve health and care
  - o CARIN is convened by Aneesh Chopra, David Blumenthal, David Brailer, and Mike Leavitt
  - o CARIN is a membership organization with nationally recognized leaders representing providers, payers, platforms, patients, and other key players
  - o The Alliance is closely engaged with Government on several priority initiatives
  - o CARIN is specifically focused on CDEx, which is different than traditional focuses on provider-to-provider exchange
- There are many drivers of change right now that make the time ripe for implementing CDEx and a Trust Framework
  - o Changes with policy help to support the rights of consumers with regards to their health information
    - 21st Century Cures sets up a right for consumers to have access to their health information in a single, longitudinal format that is easy to understand
      - Cures also lays out support from ONC to develop a Trust Framework, either in a public-public or public-private partnership that CARIN strives to become
    - There is now a clear right for the consumer through HIPPA, HITECH, and MACRA for consumers to have the legal basis to have access to their information
    - We are in a time of being able to shift from providers finding a way to deny information to consumers to a time of providers being required to share information in easily accessible ways
  - o APIs are shipping in Q1 of 2017, which will mean that EHR systems can easily share information in a safe, secure way with consumer apps
    - This creates a need for health systems to understand the risks and requirements around sharing information now

Drivers of Change

- Given the changing world of health information exchange, industry now needs to come together to get consensus on how to solve challenges and develop a framework and regulatory landscape that support consumers and protects security of information
- The Trust Framework can be based on operating principles and leverage the FTC to help enforce
    - The Trust Framework can use the example of the green button for utilities which says, as an industry, this is how we want to operate and we can make that happen

New World of CDEx

- Given that the technology now exists for information to be shipped safely and securely from an EHR to a trusted app, this exchange will need to start happening on a large scale
- The New World of CDEx can be built on the idea that a patient has a portal already and that portal information should be able to be synced with an application of their choosing
- Open Questions:
    - How do we make the information consumers receive meaningful?
    - How do we provide protections for providers that if they use a trusted API that they have a boundary for where their legal liability is should there be a breach?
    - How do we make it easier for consumers to ask for their information in the same way at different providers?
    - How do we have trusted apps that can access health information?
    - What responsibility do covered entities have once the data is authenticated to the user in an app?
    - Do apps have to be authorized every time they request information or can it be a persistent authorization?
    - How do we balance risk in the new trust framework?

Government Perspectives

- ONC, OCR, HHS, CMS, and the FTC all discussed their perspective on consumer-directed exchange
    - ONC is committed fully to the efforts of CARIN and around the Trust Framework
    - ONC is looking for ways to help be a coordinator of these efforts
    - ONC is working to develop tools for transparency around security for apps
    - OCR said the sharing of patient information is not optional
    - CMS said the current system has too much friction for consumers to get their information
    - The top concerns for CMS are not around traditional security, but how do we know what happens when consumers get their data and how does CMS know what apps to trust
    - There is a great need for a Trust Framework
    - FTC said under Section 5, FTC can bring action against those who mislead customers with regards to what happens with their health information
    - FTC has authority over apps and will use it to protect patients

Trust-Related Barriers

- Cyber security concerns and legal responsibility
- Securing transmissions
- Trusted apps
- Patient validation
- Business and brand liability if there is a breach of information
- Authorizations

Trust Framework

Group discussed various options for how to develop a consumer-directed trust framework. More discussion is needed and the group agreed to develop a workgroup to begin discussing ways to develop the framework.

Conclusion / Next Steps

- There is great energy around the need to create a trust framework now that considers the perspectives of legal, technical, providers, patients, platforms, and apps to create a system that works for all
- This group will move forward on drafting a trust framework to address all the risks/questions addressed in the meeting