The CARIN Alliance Vision

The CARIN Alliance was chartered on September 12, 2016 in Washington, D.C. with a single, unifying purpose,

"Our 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."

Since that time, we have worked with stakeholders across the health care ecosystem to achieve that goal. We want to provide an update on where we are and where we are going. We believe now, more than ever, we are closer to accomplishing our vision. We also believe we can effectively work cooperatively with consumers, caregivers, industry, and our public partners to voluntarily raise the bar on consumer privacy, security, consent, and access to health information.

Where we've been

Any time that something is proposed in health care that has never been done before, there is an extraordinary level of resistance related to business and revenue model conflict, unknown / unintended consequences, and more. As an example, during the early days of the CARIN Alliance our quarterly community meetings focused on how we could use secure and standardized HL7® FHIR® APIs called for in the 21st Century Cures Act to digitally transfer data between HIPAA covered entities and third-party applications acting on behalf of the consumer that are currently not covered by HIPAA. We envisioned a world where an individual could use their portal credentials to electronically access their health information from any application they choose while still protecting their privacy, security, and consent preferences.

Despite the requirement provided by HIPAA's individual right of access, the notion of digitally transferring protected health information (PHI) to these non-covered entities overseen by the Federal Trade Commission (FTC) was a non-starter for some. We had Chief Privacy Officers of major health systems walk out of meetings and convey serious concerns about this type of an approach. It really hampered progress during our first 12-18 months as we tried to gain consensus on a path forward.

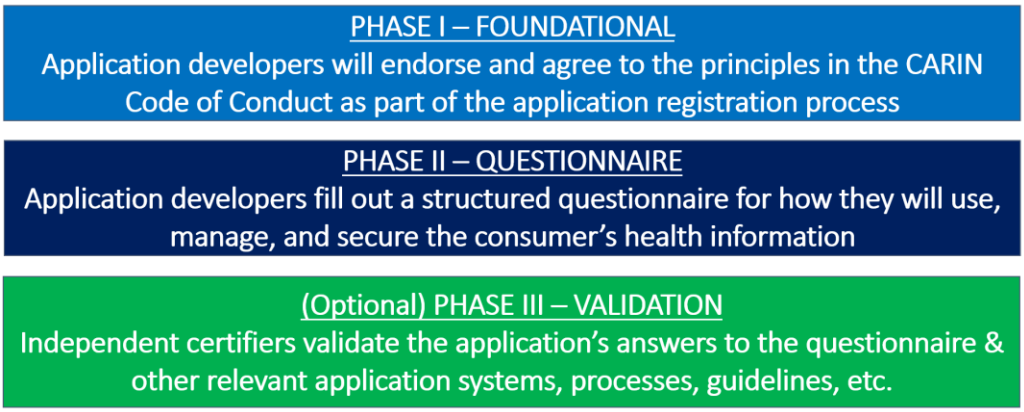
We examined all types of solutions. We looked at expanding HIPAA but that wasn't feasible for many of the reasons outlined in this recent blog post. HIPAA was designed to protect data exchange between health care entities not between health care entities and health care consumers.

- In addition, even if HIPAA could be expanded, where would that expansion end?
- Currently, the FinTech industry is focused on health and wealth. With the availability of secure and standardized HL7® FHIR® APIs, how would health care information be regulated in the financial services industry?
- Should we look to have both a regulated, mandatory HIPAA-covered data exchange world and an unregulated, voluntary, private-sector led data exchange world?
- Could we work with the private sector to help advance consumer privacy, security, and consent so future policy could account for advances in the private sector?

Our conclusion: We could develop a model where both the public and private sectors could work together to improve individual access to health information while helping to continually raise the bar on privacy, security, and consent.

The CARIN Trust Framework and Code of Conduct

The CARIN Trust Framework and Code of Conduct was released for public comment in November 2018 and officially released as Version 1.0 in May 2019. The CARIN Trust Framework involves three distinct phases:



Phase I: Foundational – The CARIN code of conduct

The Federal Trade Commission (FTC) governs all consumer-related data exchange under the protections granted under Section 5(a) of the FTC Act which provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." 15 U.S.C. Sec. 45(a)(1).

After extensive conversations with the FTC as well as other enforcement actions related to industry agreed-upon codes and pledges, we developed the CARIN Code of Conduct which is the health care industry's first agreed-upon set of best practices for how consumer health data should be handled by entities not covered by HIPAA.

It's important the industry agree to *a single set of principles* for how applications not covered by HIPAA should handle health data, protect a consumer's privacy and security, and record a consumer's informed consent preferences. Multiple codes of conduct, or myriad, divergent terms and conditions untethered from industry standards will defeat the very purpose they are trying to solve for: private sector action, FTC sanctions, or state attorney general enforcement.

We continue to seek input to our Code of Conduct and make and updates based on feedback from any and all interested stakeholders. We are also working with multiple countries and industries who are dealing with similar issues of how to share data with consumers when that data crosses between spaces governed by different regulatory regimes. This is not a healthcare-specific or US-specific issue.

Phase II: Questionnaire – Establishing a consistent user experience across platforms

Consumers are going to be accessing applications and services that can aggregate their own personal health information from many different places. They may use Apple Health if they have an iOS device, CommonHealth if they have an Android device, or any number of private sector vendors who not only will aggregate a consumer's health information but also give them insights into how they can use that data to achieve their goals.

During phase two, applications will agree to respond to a set of questions regarding how they use, manage, and secure the consumer's health data based on the principles in the code of conduct. This will include incorporating and expanding the ONC's Model Privacy Notice to be consistent with the Code of Conduct. These structured questions will allow the consumer to filter and search for the applications that meet their individual preferences across platforms. We will then take those questions and create a privacy 'nutrition label' which allows the individual user to view how each application handles their

privacy, security, and consent in a user-friendly format while maintain their ability to drill into the detail. This is a project we have actively been working on in in 2019 and will continue to work on in 2020.

Phase III: Validation – Establishing independent third-party validation for applications

Phase three allows for independent, private sector third parties to certify the applications based on the code of conduct, questionnaire, and possibly other criteria (e.g. validity of the application's clinical guidelines, etc.). We are pleased to see there are organizations who have already begun to develop those criteria.

This framework is like the work being done in other countries like the U.K. and Canada. We are talking to both of those countries and other industries like open banking which are dealing with similar issues.

Plans for 2020 and beyond

Our plans for 2020 and beyond include the following:

Involve, listen, and engage more consumer and caregiver advocates

- A subset of our board is developing a strategy to reach out, engage, and learn from consumers, patients, caregivers, and others about consumer-directed exchange and what is important to them. We have several who are already members and who have recently added their voice to ours as we encourage the OMB to release the rules "without further delay" and we hope to connect with others. Please let us know who else we can reach out to!

Update our website with a list of applications who have signed the CARIN code of conduct

- We will be updating our website with a list of consumer-facing applications who have signed our code of conduct to enable consumers, providers, caregivers, health plans, and others a common repository for those application who are willing to live by the code's higher standard.

Work to develop an intuitive, consumer-friendly 'privacy user interface'

- We want to work with other interested stakeholders, sectors, and countries on how we can develop an effective user interface that helps individuals select their privacy, security, and consent preferences against the backdrop of the CARIN code of conduct and a list of trusted third-party applications.

CARIN Blue Button® and real-time pharmacy benefit check implementation guides

- We will be balloting the CARIN consumer-directed payer data exchange implementation guide and CARIN consumer real time pharmacy benefit check implementation guide in Q1 2020 with HL7® for use by health plans, state Medicaid agencies, and others around the country to help them be in compliance with the CMS Interoperability and Patient Access proposed rule.

Digital Identity

- Find opportunities to continue to promote the creation and acceptance of NIST 800-63-3 IAL2 & AAL2 credentials for use by providers, health plans, and individuals
- Develop a set of digital identity federation principles that could be used as part of the FAL2 requirement in TEFCA
- Work to find ways to fund and/or execute multiple digital identity pilots (e.g., CMS, ONC, or other) that uses a single, person-centric federated credential across multiple health care stakeholders

We look forward to working with other interested parties on this robust set of projects to advance consumer-directed exchange for patients and caregivers everywhere.