The CARIN Code of Conduct

A foundational set of principles for how health care organizations can share data with consumer applications

Section I – Background and Overview

I. Who is the CARIN Alliance?

The CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers and caregivers. We are committed to enabling consumers and their authorized caregivers to get easy access to their personal health information. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via the non-proprietary APIs included under MACRA/MIPS and the HITECH/EHR Incentive Program, and the Promoting Interoperability objective "Provider to Patient Exchange," including the use of 2015 Edition CEHRT to have their digital health information sent to any third-party application they choose.

Working collaboratively with government leaders, the group seeks 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. With a membership composed of patients and caregiver organizations, health care entities, health information exchanges, health information technology vendors and others, the CARIN Alliance is uniquely positioned at the intersection of public and private organizations to advance the development of person-centered, value-driven health care through the adoption of consumer-directed health information exchange.

II. What is consumer-directed exchange?

Consumer-directed exchange is when a consumer invokes their individual right of access under HIPAA to request a copy of their health information from a covered entity and then directs their health information to any third party of their choice. The CARIN Alliance believes that consumer-directed exchange is an essential piece of the interoperability equation. Despite significant public and private sector investments in standards-based EHRs, and provider-to-provider health information exchange in recent years, advances in consumer-directed exchange have been limited. Most consumers still lack the ability to easily get, use, and share their digital health information when, where, and how they want using third party applications they control. Barriers to consumer-directed exchange include a lack of:

- Consensus trust, privacy and security frameworks for consumer-directed exchange
- Availability and adoption of technologies that facilitate consumer-directed exchange
- Understanding of existing policies supporting consumer-directed exchange
- Health care organizational policy or workflow barriers that may exist
- Availability of sustainable business models
- Widespread consumer education and awareness about consumer-directed exchange options

Consumer-directed exchange is fundamentally different than provider to provider data exchange because it supports sharing personally identifiable data with non-covered entities (e.g., consumer-facing applications), which are not regulated by HIPAA privacy and security rules. Data held by consumer-facing applications is governed by Section 5(a) of the Federal Trade Commission Act, which makes it unlawful for companies to engage in "unfair or deceptive acts or practices in or affecting commerce" (15 U.S.C. Sec. 45(a)(1)). "Unfair" practices are defined as those that "cause or [are] likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers

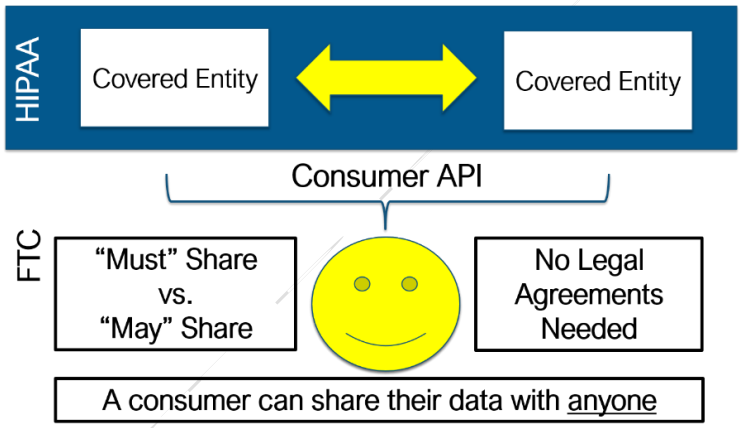
or to competition" (15 U.S.C. Sec. 45(n))". The FTC Act provides the ability for the government to hold organizations accountable for "unfair or deceptive acts or practices," and for violating commitments made to consumers regarding how their personal data will be handled.

Imagine a world where a consumer or authorized caregiver could download one or more of the thousands of mobile health applications which are available to access their digital health information from any provider, hospital, health plan, health information exchange, or other covered entity of their choosing and each of the applications would self-attest to a code of conduct and set of principles for how they will use that information. This is the focus of what the CARIN Alliance is trying to solve for.

The CARIN Alliance is primarily focused on solving two use cases:

1) How a consumer electronically **requests** access to their data, indicates where it should be sent, and is informed how their data will be used.
2) How a covered entity electronically **sends** that data to the consumer.

We are solely focused on the requirements for how health data should be exchanged outside of the blue HIPAA box below. The CARIN Alliance does not focus on data exchange within the blue HIPAA box.



While both are important and needed, there is a difference between HIPAA-related data exchange through a HIPAA Authorization and consumer-directed data exchange through an individual right of access request.

III. Individual Right of Access request vs. HIPAA Authorization

The CARIN Alliance believes that when an individual makes a request for their data to be sent to an application of their choice it should be treated as an individual 'right of access' request. We also believe that when an application makes a request for a consumer's data, it should also be treated as an individual 'right of access' request when it does the following:

- Is submitted directly by a 'personal health record' outside of HIPAA (which HITECH says is an electronic record of personal identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual)
- Meets the identity proofing and authentication requirements of the ONC's common agreement (currently Identity Assurance Level (IAL) 2 and Authenticator Assurance Level (AAL) 2)
- Clearly indicates the destination for sending the information
- Is requesting data from the HIPAA designated record set

A HIPAA Authorization request is typically initiated by a provider or other entity to document consumer consent in order to exchange data with third parties within HIPAA in circumstances where the HIPAA Privacy Rule provides no other route for disclosure (for example, where the disclosure is not for treatment, payment or operations, or under the individual's right of access).

More information on the difference between a HIPAA Authorization and an Individual Right of Access request can be found on the Office of Civil Rights website.

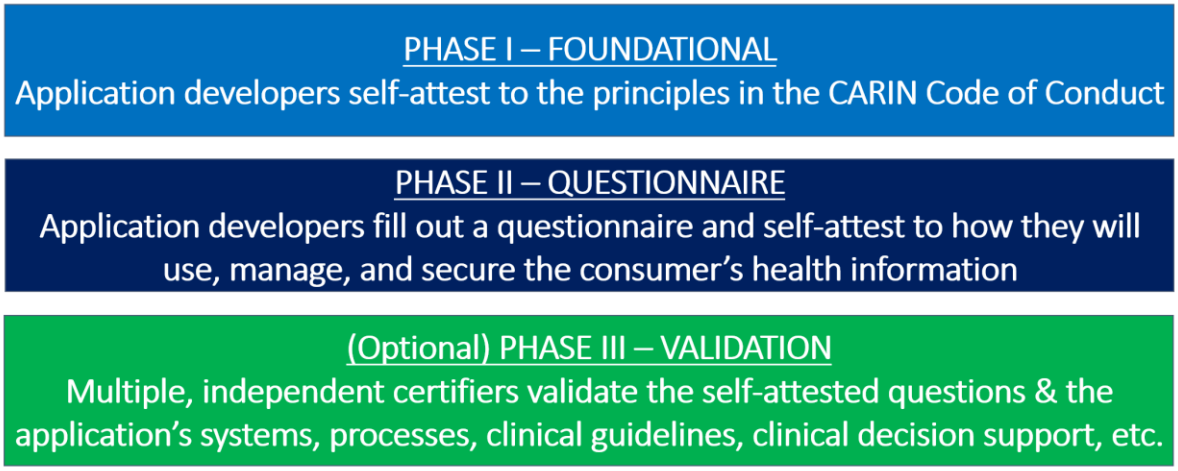
IV. Who is the audience for the CARIN Code of Conduct?

a. Consumer Advocate Groups, Consumers, and their Authorized Caregivers: Those who are looking to understand how they can electronically access their health information from multiple systems.
b. Covered Entities: Organizations that are designated as covered entities under HIPAA including providers, payers, and clearinghouses.
c. Electronic Health Record Companies: Companies that provide the technology required for providers and hospitals to keep electronic medical records data.
d. Consumer Health IT Applications: Companies who develop health IT applications for the consumer to aggregate, analyze, and share their health information including health information exchanges.
e. Non-Covered Entities: Community-based organizations, consumer platform companies, etc.

V. What is the purpose and structure of the CARIN Trust Framework?

Purpose: A consensus, voluntary framework by which health care applications that are not covered by HIPAA agree to exchange, store, and manage their personally identifiable health care information.

Structure: There are three phases of the CARIN trust framework. The CARIN Code of Conduct is phase one. This is the foundational phase where third-party application companies will self-attest to the CARIN code of conduct as part of their registration process with the "application aggregators" or primary data holders (i.e., EHR application stores, iOS or Android Application stores, etc.). During phase two, applications will self-attest to a set of questions based on the CARIN Code of Conduct for how they plan on using the consumer's health data based on the principles in the Code of Conduct. Phase three is a potential future phase where independent, private sector third-parties could certify the applications based on the code of conduct, self-attested questionnaire, and possibly other criterion (i.e., validity of the application's clinical guidelines, etc.).



VI. Who helped provide input to the CARIN Code of Conduct?

We are enormously indebted to the following organizations who have provided valuable input to the CARIN Trust Framework and Code of Conduct. These are organizations who care deeply about consumers receiving electronic access to their health information and we are incredibly grateful for their ongoing support.

Board Members
Alliance for Nursing Informatics (ANI)
Apple
The Argonaut Project / HL7
Cambia Health Solutions
Caregiver Action Network
CareJourney
Cedars-Sinai Health System
Electronic Health Records Alliance (EHRA)
Marshfield Clinic
National Partnership for Women and Families
New York Presbyterian
Alliance Members
23andMe
Aetna
Allscripts
Blue Cross Blue Shield of North Carolina
The Broad Institute
CareEvolution
Cerner
Colibrium
DaVita
GoodRx
Humana
ID.me
MedFusion
MedSavvy
Medical Home Network
Microsoft
New Jersey Innovation Institute
Security Health Plan
Surescripts
Stacey Tinianov (Patient Advocate)
Utah Health Information Network (UHIN)
Velatura / Michigan Health Information Network (MiHIN)
Special Guests / CARIN Community
American College of Surgeons
Blue Cross Blue Shield Association (BCBSA)
b.well Connected Health
Ciitizen
CVS
Digital Health Policy Advisors, LLC

Dr. First
Georgia Tech Enterprise Innovation Institute
Get My Health Data
Greenwood County Hospital
Health Care Cost Institute
Indiana Health Information Exchange (IHIE)
Imprivata
IPRD Group
LifeMed ID
Medal, Inc.
Medicare Pathfinder
New Wave Technologies
Optum
PatientLink
Point of Care Partners
Pfizer
Practice Fusion
Trinity Health
UCSF
United Healthcare
UPMC
Videntity
Walgreens
X4 Health
Affiliated Alliances
Alliance for Better Health
American Health Information Management Association (AHIMA)
The Commonwealth Fund
Commonwell Health Alliance
CHIME
The FIDO Alliance
Future of Privacy Forum (FPF)
Health Care Transformation Task Force
Health Records Banking Alliance
National Association for Trusted Exchange (NATE)
National Governors Association
HIMSS
The Pew Charitable Trusts
Sequoia / Carequality
Strategic Health Information Exchange Collaborative (SHIEC)

VII. Can we provide input to the CARIN Code of Conduct?

a. We welcome and encourage comments and input from across the health care industry. Please submit your comments online at www.carinalliance.com. The CARIN Alliance board and membership will examine and carefully consider all comments to include in future releases of this document.

Section II – The CARIN Alliance Code of Conduct

Background: The CARIN Alliance Code of Conduct represents the consensus view of a group of multi-sector stakeholders that include leading providers, payers, health IT companies, EHR companies, consumer platform companies, consumers, caregivers and others focused on advancing consumer-directed exchange across the U.S. The Code is based on internationally recognized standards including the Code of Fair Information Practices (FIP) (indicated in italics below) and numerous other consumer information sharing accepted principles and practices. The Alliance is working collaboratively with other stakeholders and leaders in government to overcome the policy, cultural, and technological barriers to advancing consumer-directed exchange**.**

The CARIN Alliance Code of Conduct

The CARIN Alliance 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. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via non-proprietary APIs. ***We envision a future where any consumer can choose any application to retrieve both their complete health record and their complete claims information from any provider or plan in the country.***

As an organization that handles personally identifiable health care information outside of HIPAA, we commit to the following regarding how we will handle personally identifiable consumer health care data.

I. Consent

The Principle of Collection Limitation, which provides that there should be limits to the collection of personal data, that data should be collected by lawful and fair means, and that data should be collected, where appropriate, with the knowledge or consent of the subject.

We will:

a) Avoid default data sharing and obtain **informed, proactive consent** from users, with such consent clearly describing how user data will be collected, used and shared.
b) Obtain separate consent (either opt-in or opt-out) to uses or disclosures for marketing purposes.
c) Comply with the Children's Online Privacy Protection Act with respect to collection, use or disclosure of data from and about individuals under the age of 13 including any applicable state laws.
d) Provide users with advanced notice of our privacy policy changes.
e) Be clear with users on how they can withdraw consent to use our service and what will happen to their data after withdrawal.
f) On behalf of our users, request a copy of their health data from the HIPAA designated record set maintained by a health care provider, health plank, or health information exchange by
    a) Requiring as an option the consumer uses technology that supports the NIST IAL2 & AAL2 standards
    b) Clearly indicating the destination for sending the health information

II. Use & Disclosure

The Principle of Use Limitation, which provides that there must be limits to the internal uses of personal data and that the data should be used only for the purposes specified at the time of collection. The Principle of Disclosure Limitation, which provides that personal data should not be communicated externally without the consent of the data subject or other legal authority.

We will:

a) Via contracts bind third-party vendors to our privacy policies and prohibit use or disclosure of user information for independent purposes absent express consent from the user.
b) Limit the collection of health information to only what the user has expressly consented that the service can collect
a) Collect, use, and disclose health information in ways that are consistent with reasonable user expectations given the context in which users provided (or authorized the provision of) the health information.

III. Individual Access

The Principle of Individual Participation, which provides that each individual should have a right to see any data about himself or herself and to correct or remove any data that is not timely, accurate, relevant, or complete.

We will:

a) Provide the ability for a consumer to access their health information on their own and/or assign access to caregivers (defined as an unpaid family member, foster parent, or other unpaid adult who provides in-home monitoring, management, supervision, or treatment of a child or adult with a special need, such as a disease, disability, or the frailties of old age) or other third-parties.
b) Establish and communicate to users clear policies with respect to health information collected by the service that may not be timely, accurate, relevant or complete.
c) Upon consumer request, securely dispose of the consumer's relevant identifiable health data completely and indefinitely to allow the consumer the right to be forgotten.

IV. Security

The Principle of Security, which provides that personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.

We will:

a) Store and retain health information in a manner consistent with industry-leading best practices that includes the highest levels of security and confidentiality.
b) Protect health information through a combination of mechanisms including, at a minimum: secure storage, encryption of digital records both in transit and at rest, data-use agreements, and contractual obligations, and accountability measures (e.g. training, access controls and logs, and independent audits).
c) Follow industry-leading safeguards for how to protect a consumer's health information against such risks as loss or unauthorized access, use, destruction, annotation, or disclosure.
d) Provide meaningful remedies for all participants involved in consumer-directed health information exchange to address security breaches, privacy, or other violations incurred because of misuse of the consumer's health information.

V. Transparency

The Principle of Openness, which provides that the existence of record-keeping systems and databanks containing data about individuals be publicly known, along with a description of main purpose and uses of the data

We will:

a) Have a privacy policy that is prominent, publicly accessible, and easy to read.
b) In that policy specify the Company's data collection, consent, use, disclosure, access, security, and retention/deletion practices, including with respect to de-identified, pseudonymized or anonymized data.
c) Provide clear updates when those practices have changed.
d) Develop privacy policies based on industry best practices to manage health data.
e) Specify in the privacy policy what will happen to a consumer's data in the event of a transfer of ownership or in the case of a company ending or selling its business, either: (i) provide users with clear option to either securely dispose of, or transmit or download their health information securely, or (ii) ensure successor entity commitments are consistent with the then-existing privacy policy.

VI. Provenance

The Principle of Data Quality, which provides that personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete, and timely.

We will:

a) Where possible, provide consumers and their caregivers with data provenance to identify who or what entity originally supplied the data and, where relevant, who made changes to the data, and what changes were made.

VII. Accountability

The Principle of Accountability, which provides that record keepers should be accountable for complying with fair information practices.

We will:

a) Designate a responsible officer within the company who is committed to these health information principles and to ensure these commitments are publicly facing to allow oversight enforcement by the Federal Trade Commission (FTC), State Attorneys General, or other applicable authorities.
b) Train our employees on these principles and ensure compliance by regularly evaluating our performance internally.
c) Be transparent with the public whether or not we have obtained independent third-party certification

VIII. Education

We will:

a) Inform consumers about their health information sharing choices and the consequences of those choices including the risks, benefits, and limitations of data sharing by providing educational materials ourselves or pointing to appropriate third-party resources.

IX. Availability

We will:

a) Actively work with data holders to expand the set of consumer health information available for reliable, consistent electronic access and to exchange with individuals, caregivers, and clinicians.
b) Actively work to expand the amount of machine-readable data to ensure a consumer can electronically access all of their health information when, where, and how they want to achieve their goals.