The CARIN Trust Framework and Code of Conduct for Consumer-Facing Applications

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

Section I–Background and Overview

- **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, open HL7® FHIR® APIs included in ONC and CMS final regulations 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 obtain, 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.

- **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 obtain, 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 has raised some concerns because it relies on sharing personally identifiable data with consumer-facing applications, many of which may not be regulated by HIPAA privacy and security rules. However, 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 companies accountable for "unfair or deceptive acts or practices," and for violating commitments made to consumers regarding how their personal data will be handled. Consumer-facing applications that qualify as "personal health records" or "PHR-related entities" are also subject to the FTC's breach notification rules, which require notification to consumers when "PHR identifiable health information" is disclosed without the data subject's authorization. Data held by consumer-facing applications also may be subject to state privacy and consumer protection laws.

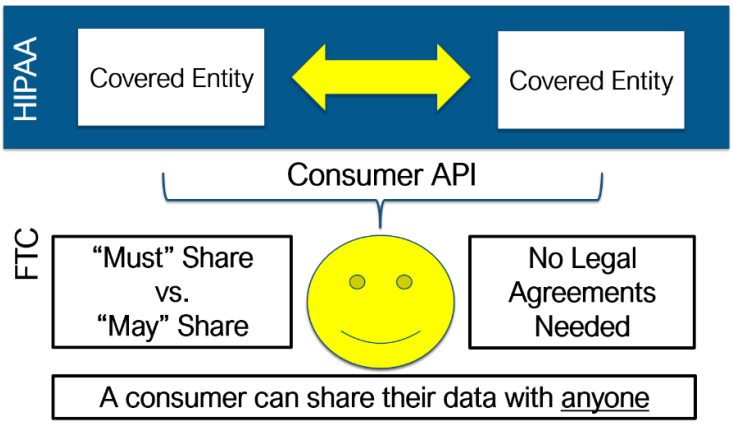
Imagine a world where a consumer or authorized caregiver could download one or more mobile health applications to access their digital health information from any provider, hospital, health plan, health information exchange, or other covered entity of their choosing. These applications would endorse and agree to the code of conduct as part of the application registration process. The FTC, through its Section 5(a) authority, could then enforce that code of conduct against apps who publicly commit to following it. The CARIN Alliance code of conduct is intended to help address the concerns associated with sharing personal health information with consumer facing apps.

The CARIN Alliance is focused on addressing the barriers associated with consumer-directed exchange, helping organizations and individuals understand existing policies supporting consumer-directed exchange, assisting health care organizations to eliminate policy or workflow barriers that may exist for consumer-directed exchange, and educating consumers on their consumer-directed exchange options.

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

1) How a consumer electronically **requests** access to their data using APIs, 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 via an application of their choice.

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



- **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 pursuant to the

HIPAA Privacy Rule. We also believe that when an application makes a request for a consumer's data at the direction of, and on behalf of, an individual, 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' (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; and
- Is requesting data from the then current U.S. Core Data Interoperability Set (USCDI).

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 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 for Civil Rights website.

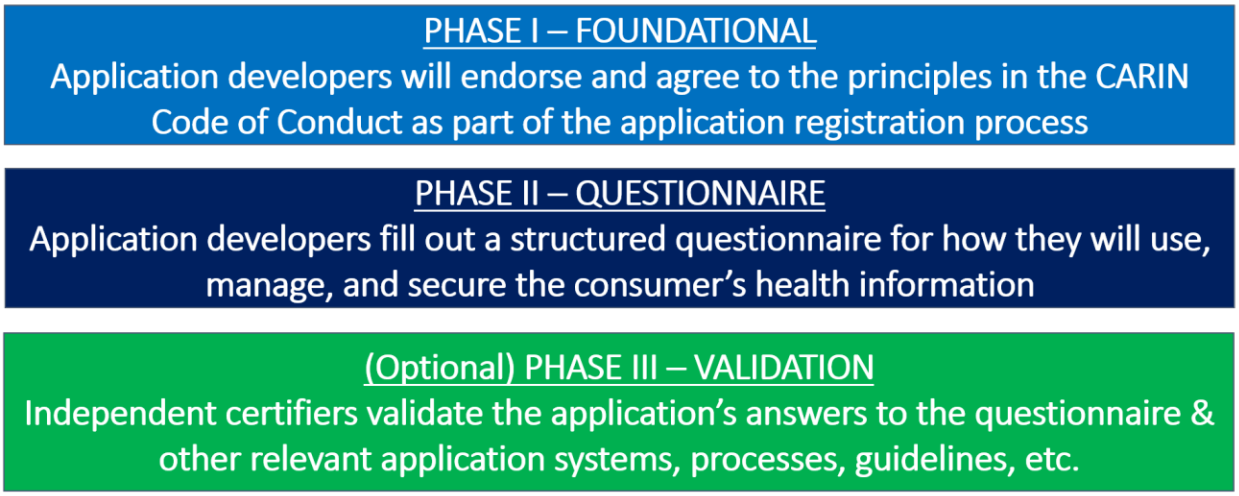
- **Who is the audience for the CARIN code of conduct?**
  a. Consumer Advocate Groups, Consumers, and their Authorized Caregivers: Those who are looking to understand how they can electronically access their health information from multiple systems.
  b. Entities covered by HIPAA: Organizations that are designated as covered entities under HIPAA including providers, payers, and clearinghouses and their business associates who operate on their behalf.
  c. Electronic Health Record Companies: Companies that provide the technology required for providers and hospitals to record clinical documentation, track workflows, and bill appropriately for care.
  d. Health Information Exchanges: Organizations who facilitate digital health information exchange on behalf of payers, providers, and consumers.
  e. Policymakers: Administration and congressional officials who are enacting health information exchange policies and procedures.
  f. Non-Covered Entities: Community-based organizations, consumer platform companies, and other entities not covered by HIPAA that develop health IT applications and/or services for the consumer to aggregate, analyze, and share their health information.

- **What is the purpose and structure of the CARIN Trust Framework?**

  Purpose: A consensus, voluntary framework by which applications used by the consumer agree to treat the individual's 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 and consumer platform companies will endorse and agree to the CARIN code of conduct as part of their registration process with the "application aggregators" or primary data holders (e.g., EHR application stores, iOS or Android Application stores, etc.). During phase two, applications will publicly endorse and agree 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. Phase three is where independent, private sector third

parties could certify the applications based on the code of conduct, questionnaire, and possibly other criteria (e.g. validity of the application's clinical guidelines, etc.). In October 2022, CARIN and EHNAC (now part of DirectTrust) announced the CARIN code of conduct accreditation program for third-party applications to become certified by an independent accreditation organization.



- **Who helped provide input to the CARIN code of conduct?**

  We are enormously indebted to the 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. For a list of those organizations, please access our website www.carinalliance.com under the section 'Our Membership'.

- **Can we provide input to the CARIN code of conduct?**

  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.

- **How does the CARIN Alliance plan on operationalizing the code of conduct?**

  The CARIN Alliance welcomes the opportunity to work with primary data holders of personally identifiable health information including health plans, the Federal Government, state Medicaid agencies, providers, hospitals, EHR vendors, HIEs, and other organizations who are implementing APIs for consumers to access their health information. We want to work with these organizations to include the code of conduct as part of their application registration process and ensure the data holders can inform consumers what applications have endorsed and agreed to the code of conduct so they can make an informed decision regarding the applications they would like to choose to access their health information.

Section II – The CARIN Alliance Code of Conduct For Consumer-Facing Applications

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) (See NCVHS report, "Health Information Privacy Around HIPAA: A 2018 Environmental Scan of Major Trends and Challenges, p.19) and numerous other 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 envisions a future where any consumer can choose any application or service to retrieve both their complete health record and their complete claims information from any provider or health plan in the U.S. and have that information used, managed, and stored by a third-party application based on the individual's consent and personal preferences.

Application: The CARIN Code of Conduct for Consumer-Facing Applications is meant to apply to *all* consumer-facing applications (see definition below) that are offered to and used by consumers in the United States, regardless of whether or not they are covered by HIPAA. The Code of Conduct applies to a Consumer-Facing Application (CFA) prospectively from the date the CFA signs onto Code unless the CFA indicates otherwise in publicly accessible materials.

Definitions:

- Consumer-Facing Application (or CFA): technology enabled platforms, services and tools that, on behalf of the individual, can draw personal data from multiple sources and that is managed, shared, and controlled by or primarily for the individual user/data subject.
- Personal Data: Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Data (or Information): Any information relating to a natural person (including personal data, de-identified information, and pseudonymized information).
- De-identified Data:
    - Data that meets one of two criteria:
        - (1) Data that cannot reasonably be linked to an identified or identifiable individual and the entity that controls the use and disclosure of the data:
            - (A) Takes reasonable measures to ensure that the data cannot be associated with an individual;
            - (B) Publicly commits to maintaining and using the data without attempting to re-identify the data; and
            - (C) Obligates any recipients of the data through contractual requirements to take reasonable measures to ensure that the data cannot be associated with an individual and to not attempt to re-identify the data; or
        - (2) Information that has been deidentified in accordance with 45 C.F.R. § 164.514(b) of the regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and was derived from protected health information that was subject to HIPAA.
- Pseudonymized Data: Data that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the data is not attributed to an identified or identifiable individual.
- Use: Use means, with respect to personal data, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
- Disclosure: Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

- Consent: Statement or a clear affirmative action from a data subject authorizing the use or disclosure of his or her personal data after being given full information about the means by and purpose of any such uses or disclosures, and the possible effects or results of providing such authorization.
- Health Data: Personal data related to the physical or mental health of a data subject, including the provision of health care services, which reveal information about the data subject's health status.
- Targeted Advertising: Displaying an advertisement to a user of a CFA where the advertisement is selected based on personal data obtained from the CFA or from health data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.
- Automated decision-making: Means a decision made by the offerer of the CFA that results in the provision or denial by the CFA offeror, or an entity with which the CFA offeror shares personal data, of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

The CARIN Alliance Code of Conduct for Consumer-Facing Applications

This CARIN Alliance Code of Conduct is meant to provide consumers with transparency into how their information is being used and disclosed by their chosen CFA(s).

As an offeror of a CFA, we commit to the following:

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

I. **Transparency**

We will:

a) Have a privacy policy that is based on industry best practices and is prominent, publicly accessible, and easy to read (i.e., written in lay language) and that, along with related notices and other materials that are consumer-facing and affirmatively offered to and easily accessible by consumers, addresses all of the issues addressed in the code of conduct..
b) Ensure our privacy policy, related notices, and/or other consumer-facing materials provide information on our Company's data collection, consent, use, disclosure, access, security, and retention/deletion practices, including the use and disclosure of personal data as well as of de-identified, or pseudonymized information.
c) Be clear with users which uses and disclosures are conditions for use of the CFA and which are at the option of the user, which require offerors of CFA to provide users with the option to decline to use their personal data for marketing or automated decision-making.
d) Address in our policy when personal data disclosure could have an impact on individuals other than those requesting their information through the application (such as the impact of disclosing genetic or family history information on relatives of requesting individuals).
e) Proactively provide clear updates to users when privacy policies or practices have changed.
f) Use the ONC's Model Privacy Notice (MPN) and the CARIN questionnaire as a resource when developing the privacy policies of the application.
g) Be clear with users regarding whether personal data are collected, or are disclosed to third parties, on a one- time basis or persistently collected (and if so, for what duration) and allow the user rights to change those options consistent with our consent policies.
h) Be clear with users regarding their rights (or lack thereof) to change or annotate personal data or to disclose portions of their personal data and whether any such changes, annotations, or notices of lack of completeness are communicated to any downstream recipients authorized by the user.

i) Explain what will happen to the user's personal data after they withdraw their consent.
j) Explain whether data subjects have the right to have their personal data deleted, and if so, how a data subject can exercise this right. Specify in the privacy policy what will happen to a user's personal data in the event of a transfer of ownership or in the case of a company ending or selling its business, and provide the user with at least one of the following options: (i) securely dispose of, transmit, or download their personal data, (ii) ensure the successor entity commitments are consistent with the organization's then-existing privacy policy, or (iii) allow the user the option to close their account.
k) Privacy notice should describe any use and disclosure of personal and/or health data for targeted advertising purposes.
l) Privacy notice should describe any use and disclosure of data for automated decision-making in ways that produce legal or similarly significant effects on a consumer, and the developer's consent practices with respect to these purposes. Be clear with users regarding our policies regarding dormant or closed accounts.

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 data subject.

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.

II. Consent

We will:

a) Avoid default personal data sharing by obtaining **informed, proactive consent** from users in advance of personal data disclosure with such consent clearly describing how user personal data will be collected, used and disclosed.
b) Obtain separate, informed, proactive opt-in consent to use or disclose personal data from any individual or other individual identified in the personal data for marketing purposes. (For example, Individual A's consent does not extend to Individual B who may be referenced in Individual A's personal data.) With respect to targeted advertising, developer shall obtain separate proactive consent as consistent with the requirements noted in II(b).
c) Comply with the Children's Online Privacy Protection Act that is defined by applicable law.
d) Provide users with advance notice of material changes to our privacy policy and allow the user to affirm their consent to the updated privacy policy changes in order to continue to use and disclose their personal data with the application or give user the option to withdraw consent or close the account.
    - "Material change" means a change that results in the use and disclosure of personal data by Company in a different manner than when the personal data was collected or otherwise obtained that user's should be made aware of before the use and disclosure occurs. This includes, for example, changes that may adversely affect the user, new categories of personal data processed by Company, or any change to how personal data is processed by Company that a user may not reasonably expect (e.g., use and disclosure of existing personal data collected by Company for new or different purposes).
e) Provide users with an easy process for how to withdraw an optional consent to personal data uses and disclosures and clearly communicate that process to users.
f) Allow the user to always indicate any third-party recipients to whom their personal data are to be shared through the CFA or through other appropriate means.

The Principle of Use Limitation, which provides that there must be limits to the 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.

III. Use & Disclosure

We will:

a) Contractually bind third-party vendors and contractors to the commitments we make to users, in substantively similar language, regarding use or disclosure of user data (pursuant to Section 1b of the Code) and prohibit uses or disclosures of user data for any purposes not consistent with those commitments without informed, proactive consent from the user.
b) Except for the contracted third-party vendors identified above, or as required by law, prohibit the use or disclosure of user personal data without user consent.
c) Limit the collection of personal data to only what the user has expressly consented that the application can collect.
d) Collect, use, and disclose personal data in ways that are consistent with reasonable user expectations given the context in which the users provided (or authorized the provision of) the health information, as described in the user consent.

The Principle of Individual Participation, which provides that each individual should have a right to see any data about himself or herself and to annotate any data that is not timely, accurate, relevant, or complete where the application has the ability to do so.

IV. Individual Access

We will:

a) To the extent technically feasible and where consistent with applicable law, provide the ability for users to access all personal data about the user collected by the application.
b) Provide a clear and easy process to enable users to report any suspected inaccurate or incomplete data.
    - To the extent technically feasible, identify whether the error was in the personal data obtained from another source or is an error inserted by the CFA,
    - Educate users on their rights to request corrections to medical records from entities covered by HIPAA, and
    - To the extent technically feasible, and in any case where required by law, appropriately address any error or incompleteness that is the responsibility of the CFA.
c) Establish and clearly communicate to users clear policies for how the application will handle personal data it collects that may not be timely, accurate, relevant, or complete.
d) Upon user request, provided that Company is not legally required to retain a user's personal data and to the extent technically feasible, securely dispose of the user's personal data completely and indefinitely to allow the user the "right to be forgotten" with respect to any future uses or disclosures of user's personal data.

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.

V. Security

We will:

a) Follow safeguards consistent with the responsible stewardship associated with protection of a user's personal data against risks such as loss or unauthorized access, use, alteration, destruction, unauthorized annotation, or disclosure.

b) Store and retain personal data in a manner consistent with the best practices associated with the protection of personal data.

c) Protect personal data 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/or contractual obligations imposed on third party recipients of personal data (e.g., cloud vendors), and accountability measures (e.g., access controls and logs and independent audits) appropriate for the personal data held by Company that could be made available to the user.

d) Comply with applicable breach notification laws and provide meaningful remedies to address security breaches, privacy, or other violations incurred because of misuse of the user's personal data.

e) On behalf of our users and as applicable, request a copy of their health data from the HIPAA designated record set maintained by a health care provider, health plan, or health information exchange by 1) relying on a health care provider or health plan portal identity credential using SMART or accept a digital identity credential for the user that is at least NIST Identity Assurance Level 2 (IAL2) and Authenticator Assurance Level 2 (AAL2) and 2) clearly indicating the destination for sending the personal data.

f) Adopt internal policies and secure contractual commitments with third parties to prohibit the re- identification of de-identified or anonymized data.

g) Establish and implement a policy for how to handle dormant user accounts.

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.

VI. Provenance

We will:

a) Where possible, as data are changed, continue to maintain the provenance of the data to provide users, their caregivers, and authorized recipients information about who or what entity originally supplied the data and, where relevant, who made changes to the data, and what changes were made.

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

VII. Accountability

We will:

a) Comply with all applicable federal and state laws.

b) Designate a responsible executive officer within the company who is committed to these data principles and ensure these commitments are publicly facing to allow oversight enforcement by the Federal Trade Commission (FTC), State Attorneys General, or other applicable authorities.

c) Establish and clearly communicate a process for collecting and responding to user complaints.

d) Train our staff on these principles and ensure compliance by regularly evaluating our performance internally.

e) Notify the public when we have received any certification or accreditation from any independent certifying organizations (and indicate the timing/duration of such certifications).

In addition to the above commitments that give meaning to the Code of Fair Information Practices, we agree to support the vision of the CARIN Alliance as follows:

VIII. Education

We will:

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

ATTESTED BY:

Company	
Chief Executive Officer (Print)	
Chief Executive Officer (Signature)	
Date	