CONSUMER-DIRECTED EXCHANGE – TRUST FRAMEWORK PRINCIPLES AND BEST PRACTICES

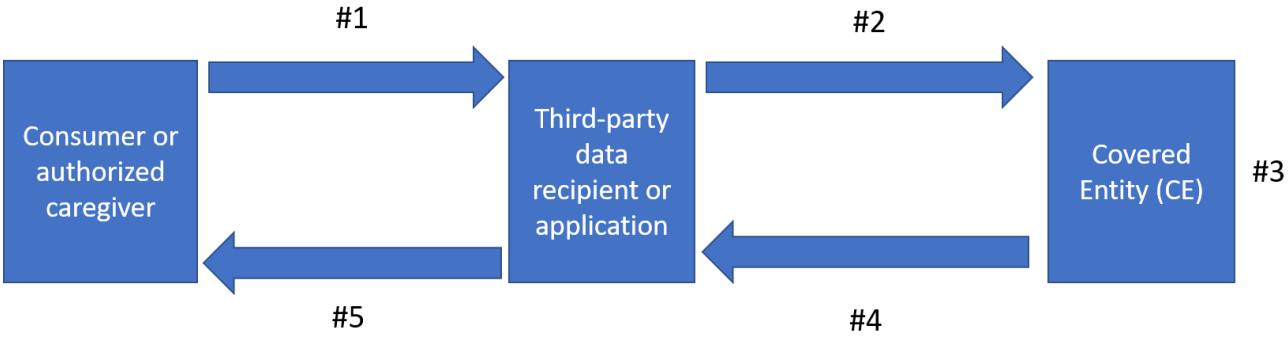
WORKING DOCUMENT

CARIN Trust Framework Principles

**Approved by the CARIN board on 5/3/17 **

I. BACKGROUND

Consumer-directed exchange occurs when a consumer or an authorized caregiver invokes their HIPAA Individual Right of Access (45 CFR § 164.524) and requests their digital health information from a HIPAA covered entity (CE) via an application or other third-party data steward.



The following principles and best practices are primarily focused on the following process:

Step #1: Consumer makes a request under their individual right of access (implied or explicit)
Step #2: Consumer names an application to be their data steward.
Step #3: Covered entity adds requested data to API server.
Step #4: Covered entity authorizes application with token that is associated with the consumer.
Step #5: Application queries covered entity API server for data.

This document is constructed to provide a set of tools for consumers, their authorized caregivers, covered entities, and third-party data stewards or applications to use to help implement digital consumer-directed exchange and will ultimately include the following sections:

- A set of consensus-driven, industry **guiding principles** for trusted consumer-directed data exchange
- **Major topics** related to consumer-directed exchange including questions industry feels needs to be addressed
- Within each major topic, **use cases** that provide **best practices** for organizations who are facilitating consumer-directed data exchange

II. GUIDING PRINCIPLES

The Consumer – Our Governing Principle

1. **Consumers Right to Access, Store, Share and Use:** Consumers or their authorized caregivers have a right to access, share and receive their available digital health information. They can provide access to any third-party data steward they authorize. The digital health information will be provided in any readily producible format they request, in as close to real-time as feasible, and at no cost.

Principles for Covered Entities

1. **Access for consumers.** Covered entities have a responsibility to provide consumers or their authorized caregivers access to share their available digital health information with any third-party data steward when a consumer invokes their individual right of access.

2. **Consumer authentication.** Covered entities authenticate the identity of the consumer or authorized caregiver requesting access to their digital health information before providing access.

Principles for Data Stewards including third-party applications and EMR/HIT vendors

This applies only to data stewards which are third-party applications provided by non-covered entities

1. **Openness and transparency.** Consumers should be able to know what personal information has been collected about them, the purpose of its use, who can access and use it, and how it is shared. They should also be informed how they may obtain access to information collected about them and how they may control who has access to it. Data blocking is not acceptable.

2. **Purpose specification.** The purposes for which personal data is accessed by the third-party data steward should be specified at the time of collection and subsequent use should be limited to those purposes, unless otherwise authorized by the consumer.

3. **Use limitation.** Personal data should not be disclosed, made available, or otherwise used for purposes other than those proactively specified by the consumer. Information should be clearly spelled out regarding how the application will access, use and share the data on the consumer's behalf.

4. **Data quality and integrity.** Data provenance should be provided where possible to identify who originally supplied the data and if there were any changes, who modified the data when.

5. **Security safeguards and controls.** Robust safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure. Consumers can use any application of their choice.

6. **Accountability and oversight.** Data stewards in possession of personal health data will be held accountable for implementing these principles. Covered Entities will not be involved in the oversight of third-party applications.

7. **Remedies.** Meaningful remedies must exist for all participants involved in the data exchange to address security breaches, privacy or other violations incurred as a result of misuse by the application.

8. **Endorsement and Certification.** Data stewards should have the ability to obtain endorsements and/or certifications from independent organizations.

9. **Openness and completeness of data sharing.** Health IT developers should actively seek ways to expand the set of patient data available for electronic access and exchange with individuals, patients, caregivers, and clinicians. Ultimately, machine-readable data should be expanded to ensure the entire health record is available electronically to the individual who requests it.