August 25, 2017

Dr. Don Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: 21st Century Cures Act Trusted Exchange Framework and Common Agreement Public Comments

Dear Dr. Rucker:

On behalf of the CARIN Alliance, we want to thank you for providing the opportunity to comment on the Office of National Coordinator's (ONC's) work to develop a Trusted Exchange Framework and Common Agreement in conjunction with the 21st Century Cures Act. We appreciated the opportunity to participate in the July 24, 2017 kickoff meeting in Washington, D.C. and look forward to further participation in the weeks and months ahead.

As you are aware, 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 open APIs mandated under MIPS/Stage 3 Meaningful Use (MU) ACI objectives and the use of 2015 Edition CEHRT to have that information sent to any third-party application they choose.

In summary, we believe the following

- Electronic provider-to-consumer health information provision is required under the law, upon request, therefore helping to expedite health information sharing with consumers and third-party applications they designate.
- Consumer-directed exchange supports sharing of personal health information with non-covered entities which are not regulated by HIPAA and therefore not subject to the same privacy and security rules as providers, plans and clearinghouses
- Consumers and their authorized caregivers should easily be able to get, use, and share their digital health information when, where, and how they want to achieve their goals.
- One of the most important issues to solve to advance consumer-directed exchange and promote widespread adoption is the ability to remotely identity-proof individuals across systems. We have a number of ideas for how to do that and look forward to working with the ONC to further discuss.

Thank you again for your consideration of our comments and recommendations. If you have any questions, please feel free to contact me at ryan.howells@leavittpartners.com.

RH Ryan Howells

Ryan Howells
Principal, Leavitt Partners
The CARIN Alliance

I. BACKGROUND ON THE CARIN ALLIANCE

The CARIN Alliance is a non-partisan, multi-sector alliance convened by David Blumenthal, David Brailer, Aneesh Chopra, and Mike Leavitt, formed in 2016 to unite industry leaders in advancing the adoption of consumer-directed exchange across the U.S. 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 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.

The Alliance is operated by Leavitt Partners and is a membership-based organization. It operates as a 'coalition of the willing' inviting all interested parties to participate and contribute. The Alliance is governed by a Board of Directors who are organizations directly involved in care, administration or consumer advocacy, including providers, health systems, payers, and consumer advocates. The Board of Directors governs the Alliance and sets the mission, strategy, policy, and activities of the Alliance. Within this structure, the CARIN Alliance is open to participation by any organization who is working to achieve the vision of consumer-directed exchange.

CARIN's 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.

To achieve our goals, the Alliance is guided by the following principles:

- **Collaboration** – Empower consumers and providers to partner in healthcare decisions at every level, wherever the consumer seeks care.
- **Availability** – Make consumer health information easy to get, use, and share by consumers and their care teams
- **Usability** – Make consumer health information digital, valuable, and intuitively understood by the end user
- **Multi-platform** – Use an ecosystem of innovative platforms while remaining platform agnostic
- **Consensus Standards and Frameworks** – Support open industry standards and frameworks
- **Security and Privacy** – Support privacy policies that align with effective cybersecurity protocols and systems

To achieve our vision, the CARIN Alliance leverages three key strategies.

- **Organize "Learning Laboratories" –** Learning labs will allow member organizations who are actively facilitating a consumer's ability to get, use, and share their health information a platform to partner with others
- **Develop and promote best practices** – CARIN will provide opportunities for members to share lessons learned and develop best practices for advancing consumer-directed exchange
- **Educate, advocate, clarify, and develop policy –** CARIN's regulatory and legislative policy dissemination and development efforts will support Consumer-directed exchange and help remove barriers to adoption.

In addition to full Alliance membership, the CARIN Alliance opens itself to comments from the public, both on documents and through open community meetings. The Alliance also posts all its deliverables, frameworks, and documents on www.carinalliance.com for public consumption. The work of the Alliance is vendor and

technology agnostic. The Alliance strives to develop best practices, guidelines, and templates that can be used regardless of which technology an entity is using. The CARIN Alliance is focused on encouraging the use of open standards and technologies where possible. The Alliance does not develop standards, but promotes consensus frameworks and open standards that support its vision.

In the world of interoperability and electronic health information exchange, much of the conversation and policy efforts have focused on provider to provider exchange – often leaving the consumer, patient, and their authorized caregivers out of the conversation. Provider to provider electronic provision of health information is not required under the law in the same direct way as is provider to consumer under HIPAA and is also regulated by the privacy and security policies associated with HIPAA. This type of data exchange is not a focus of the Alliance. The CARIN Alliance exclusively addresses provider to consumer data exchange that requires a provider to deliver health information to a consumer or their authorized caregiver in any readily producible form the consumer requests. More specifically, we are focused on a streamlined and trusted way for consumers to have their electronic health information held by covered entities be accessible by third-party applications of the consumer's choice, using the APIs as set forth in relevant regulations including MIPs and the ONC 2015 edition CEHRT.

II. CONSUMER-DIRECTED EXCHANGE

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. While view, download, and transmit functionality began to move the ball forward, more work is needed to make the experience easier on the consumer. Barriers to consumer-directed exchange include a lack of:

- Widespread consumer education and awareness about consumer-directed exchange options
- Availability and adoption of technologies that facilitate consumer-directed exchange
- Understanding of existing policies supporting consumer-directed exchange
- Organizational policy or workflow barriers that may exist
- Availability of sustainable business models
- Consensus trust, privacy and security framework(s) for consumer-directed exchange

Consumer-directed exchange is fundamentally different than provider to provide data exchange as it supports sharing with non-covered entities which are not regulated by HIPAA privacy and security rules. Non-covered entities will receive digital information and can make it available directly to consumers and others they designate through consumer-facing applications. In the future, consumers will be able to choose and direct their information to applications. While any consumer can walk into any doctor's office in the country today and request their health information, in digital form if available, we currently do not have the ability to seamlessly transmit digital health information from one or more than one system to one or more than one application with consumer's digital consent. Imagine a world where a consumer or authorized caregiver could download one of more than 165,000 mobile health applications[1] and access their digital health information from any provider or hospital of their choosing. That's what the CARIN Alliance is trying to solve.

[1] http://www.imshealth.com/en/thought-leadership/quintilesims-institute/reports/patient-adoption-of-mhealth

The world of consumer-directed exchange is already well supported by HIPAA and other efforts that have paved the way and made clear that consumers have a right to access and share their data. This type of sharing is no longer optional for providers or plans, and setting up the necessary infrastructure to support this right is key to this vision becoming a reality.

Enabling Policy
HIPAA
What it Does: Requires covered entities to share health information with consumers and/or their designated agents upon request within 30 days What it Does Not Do: Eliminate provider option to require patients to sign paper authorizations
HITECH
What it Does: Authorizes ONC to define interoperability standards, certify technologies, and provide funding to support use of certified technologies What it Does Not Do: Roles and responsibilities of "trusted intermediaries" such as consumer authorized applications
MACRA/MIPS
What it Does: Requires clinicians to attest to not participating in information blocking; strengthens ONC authority to set standards; requires providers to provide patient access to their health information via APIs in the Advancing Care Information performance category as part of the Quality Payment Program What it Does Not Do: Specify how to define information blocking
21st Century Cures
What it Does: Strengthens consumer rights to access, use and share their data; strengthens laws prohibiting health information blocking; encourages consumer-directed sharing to support research. What it Does Not Do: Specify details of how these directions should be implemented.

III. CARIN ALLIANCE TRUST FRAMEWORK GUIDING PRINCIPLES

Background

The CARIN Alliance identified the need for a trust framework to support consumer-directed exchange as a top priority for members in September 2016. In the Fall, we did landscape research, gathered input from multiple stakeholders in several separate meetings and organized a major CARIN Trust Framework kick-off event in December 2016. The meeting included several government leaders who briefed the group on relevant laws and regulations. We then held a series of follow-up meetings in 2017, drilling down on technological, policy-related, business and process-related considerations. The board and community discussion include key aspects of a trust framework including stakeholders, technology, workflows, policy, and enforcement. The community elected to focus initially on developing a high-level set of guiding principles for developing a consumer-directed exchange trust framework.

Why is a trust framework needed for consumer-directed exchange?

Until recently, health information exchange frameworks in the U.S. has primarily focused on sharing personal health information (PHI) between providers, plans, clearinghouses and their business associates (HIPAA Covered Entities), to support activities of treatment, payment and operation as defined under HIPAA. However, because of recent technological advances and regulatory clarifications, a new class of consumer-directed applications are now entering the market designed to access, store and re-share data on behalf of consumers. As discussed in *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA,* a 2016 letter from HHS to Congress, these new kinds of applications are not regulated by HIPAA or many other health information privacy or security laws.

Furthermore, laws and guidelines enabling use of consumer applications have recently been strengthened. The Office of Civil Rights has clarified that, per the HIPAA individual right of access, a consumer has the right to have their data sent to any application they choose in any "readily producible format" they request. And new rules in MACRA and 21st Century Cures prohibiting *health information blocking* by providers, EHRs and other covered entities further strengthen the ability for consumers to choose which applications access their data.

As also discussed in the 2016 letter to Congress, the FTC is the appropriate jurisdiction for regulating consumer-directed applications. FTC, Section 5, regulates unfair or deceptive acts or practices in or affecting commerce, and has begun the process of looking at how to regulate these new types of applications. Voluntary, consensus-based trust frameworks provide the ability for consumer-directed exchange. Once an application agrees to abide by the principles within a trust framework and incorporate the terms of services it requires, it may be subject to enforcement action by the FTC as well as action by private-sector bodies involved in overseeing the application community.

Research and Sources

In developing our trust framework principles and recommendations, we reviewed and analyzed a range of relevant documents. In doing so, we sought to avoid duplicating any work already performed and to leverage best practices that may exist. While not exhaustive, the documents we reviewed included the Markle Foundation's Connecting for Health *Common Framework* (2006), the Sequoia Project's DURSA and Carequality frameworks, The National Institute for Standards and Technologies publications including its *Developing Trust Frameworks to Support Federated Identities,* the Application Programming Interface (API) Task Force Recommendations (2016), Letter to Congress, July 2016, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, by ONC and FTC, Health Record Banking Alliance standards and recommendations for consumer-facing data aggregation services, ONC-related documents on consumer-directed exchange, the ONC Model Privacy Notice, Office of Civil Rights publications on HIPAA individual right of access rights, the Federal government Health IT strategic plan, the Get My Health Data initiative, relevant sections of HIPAA, HITECH, MACRA, 21st Century Cures, FTC Section 5, and related regulations. We reviewed documents developed by researchers at University of Louisville analyzing and recommending approaches for a consumer-directed exchange trust framework, under support by the Commonwealth Fund (publication forthcoming).

THE 12 PRINCIPLES OF CONSUMER-DIRECTED EXCHANGE

The CARIN Alliance reached consensus on 12 guiding principles to support consumer-directed exchange. These were approved by the board in May, 2017 and published on the CARIN Alliance website. Listed below is each principle followed by a brief rationale on why the principle is important.

RECOMMENDATION TO ONC: The CARIN Alliance recommends the ONC reflect the intent of these 12 guiding principles as part of the use case within the trust framework and common agreement that is focused on consumer-directed exchange.

The consumer – our governing principle

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.

Rationale: This principle clearly defines the overarching rights of consumers and their authorized caregivers to access, store, share and use their digital health information in any way they wish that is feasible for data stewards to support. Its importance lies in making it clear that all data stewards have a responsibility to provide data to consumers and their designees upon request in any way they request the information.

Principles for covered entities

Principle 2. 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.

Rationale: This principle delineates the responsibility of covered entities to consumers and their third-party designees with access to their data up request. Its importance lies in clarifying that covered entities have a responsibility to share data with authorized third-party designees upon request.

Principle 3. Consumer Authentication. Covered entities authenticate the identity of the consumer or authorized caregiver requesting access to their digital health information before providing access.

Rationale: This principle clarifies that covered entities have the right and obligation to identity of a consumer or authorized caregiver before providing access. Its importance lies in clarifying that covered entities have a right and responsibility to use reasonable measures to identity-proof and authenticate users before releasing data to a third-party application.

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

These apply to data stewards which are third-party applications provided by non-covered entities and EMR/HIT vendors

Principle 4. 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.

Rationale: This principle sets forth obligations for third party data stewards to be open, transparent and not engage in any form of data blocking with respect to consumers. Its importance is to provide clarity regarding these responsibilities.

Principle 5. 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.

Rationale: This principle requires a description of the purpose of data collection and limits the ability of applications to use it for other purposes without authorization by the consumer. For example, an application which collected data for purposes of asthma care may not turn around and sell it to an advertising firm without consumer consent. Its importance lies in informing consumers about how applications will use their data.

Principle 6. 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.

Rationale: This principle requires applications to describe how they will access, use and share a consumer's data. For example, if an application plans to re-share data with external third parties, that should be so stated. Its importance lies in informing consumers about how their data will be used or shared with parties.

Principle 7. 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.

Rationale: This principle requires applications to keep track of the sources of each data element, of any changes made to it, and who made the changes, and of providing that information to consumers and others with whom it may be shared. It is important because the quality and value of data used to support health decision-making depends significantly on understanding where it comes from, whether it has been modified, and who has modified it.

Principle 8. 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.

Rationale: This principle requires applications to use robust safeguards to protect personal data from risks of loss, unauthorized access, disclosure, and so on. Its importance lies in the significant risks of data loss that can occur in today's environment, whether through malicious actors, or operational sloppiness. Robust controls will help protect consumers and applications from those risks.

Principle 9. 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.

Rationale: This principle calls for data stewards to be held accountable for implementing these principles. This accountability, however, may need to be voluntary in nature. Any application authorized by a consumer may have the right to access any data requested. With this exception, covered entities should not be expected to oversee or "curate" which applications access their systems. Application selection should be left solely to the discretion of the consumer.

Principle 10. 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.

Rationale: This principle calls for meaningful remedies to be in place for all parties involved in sharing data, in the event of problems. Its importance lies in defining the need for good governance, and fair process, to be used for making decision about inclusion or exclusion of any party from an exchange network.

Principle 11. Endorsement and certification. Data stewards should have the ability to obtain endorsements and/or certifications from independent organizations.

Rationale: This principle is designed to empower data stewards to obtain and share endorsements and certifications – think "good housekeeping seals of approval" – for their capabilities. Its importance is that it makes it possible for many parties to develop and provide objective endorsements and certifications for different applications. These can then be viewed to help consumers make decisions about which applications they wish to use and trust. They can also be used by the EMR or provider to determine what capabilities beyond simple consumer access that a consumer application might be granted.

Principle 12. 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.

Rationale: This principle encourages developers to move as quickly as possible to making comprehensive, machine-readable health data available when, where and how it is wanted by consumers and all who serve them. Its importance is in encouraging action by developers to advance robust interoperability for data-stewards as quickly as possible.

IV. CARIN ALLIANCE USE CASES

Within the CARIN Alliance, we are focused on two key use cases to advance consumer-directed exchange:

Use Case 1: Consumers or their authorized caregivers can select a third-party application of their choice and invoke their individual right of access to provide consent to electronically transmit their data from one or more than one provider to their desired application

Within this use case, we are looking for ways for consumers and their caregivers to be able to invoke their right of access to their own health information using electronic means. Specifically, we are working on looking at model privacy notices and ways for patients and their caregivers to be easily and seamlessly be able to invoke this right that HHS OCR has made clear.

For consumers and their authorized caregivers to access their health information, they need to invoke their individual right of access under HIPAA. According to the Office of Civil Rights, a consumer or their authorized caregiver can invoke their individual right of access by simply verbally requesting their information from a provider of their choosing. In 21st Century Cures, the law states that individual right of access requests must be fulfilled 'without any undue effort'. We wholeheartedly believe consumers should have the right to request their digital health information in ways that work best for them. This may include in-person verbal requests,

remote requests via phone, or electronic communications like text or email, or directly through third-party applications.

There are two ways consumers can request access to their information:

- Access the information for themselves
- Access the information as a personal representative or authorized caregiver for someone else

A Release of Information (ROI) Authorization may be distinct from standard individual right of access methods, in that it is requested by patients (or their personal representative) to release their information to some other third party. ROI requests are not specifically within the scope of the CARIN Alliance.

Listed below are various ways in which a consumer / patient could provide consent to access their data.

Method	**Solutions to Consider**
Patients who already have a 'tethered portal' account	SMART on FHIR
Patients who do not have a 'tethered portal' account	Two options: • Providers will ask their patients to go through the portal to create a UN/PW and then use SMART on FHIR • Development of a remote ID proofing solution that would be developed as an open standard to be used in conjunction with SMART on FHIR
Personal representatives who already have a 'tethered portal account' for the patient they represent	SMART on FHIR
Personal representatives who do not have a 'tethered portal account' for the patient they represent	Two options: • Providers will ask their patients to go through the portal to create a UN/PW and then use SMART on FHIR • Development of a remote ID proofing solution that would be developed as an open standard to be used in conjunction with SMART on FHIR
Providers who do not wish to offer a portal and only offer API access	Two options: • Providers will provide the patient request for health information model form or something similar for patients to request their health information • Development of a remote ID proofing solution that would be developed as an open standard to be used in conjunction with SMART on FHIR

For the last option although not ideal, we believe providers across the country can use an analog-to-digital process for requesting their health information similar to a HIPAA authorization form. CARIN has supported and promoted the work of the Association of Health Information Management Association (AHIMA) and their paper-based patient request for health information model form. Currently, when consumers arrive at a doctor's office they are presented with a HIPAA authorization form to allow their provider to share the patient's information with other providers as part of their treatment. For providers who do not wish to offer a portal and only offer API access, we believe those provider offices should provide a form that provides an opportunity for the consumer to request their health information.

RECOMMENDATION TO ONC: The CARIN Alliance encourages the ONC to work closely with AHIMA to promote the patient request for health information model form as an initial first step for all providers to use to educate patients on their right to request their health information when a portal is unavailable.

The CARIN Alliance is currently working with the open standards community to develop a common approach for how a consumer can provide digital consent through the application of their choice.

RECOMMENDATION TO ONC: The CARIN Alliance believes as part of a common agreement and trust framework the ONC should support common, open standard approaches for how consumers and their authorized caregivers can digitally request access to their health information via an application or third-party data store of their own choosing.

From our discussion within the CARIN Alliance, we believe at a minimum the digital request should include the following:

1. The ability to **ID proof the consumer and authorized caregiver** who is making the request to ensure that each party involved is able to verify that the person is who they say they are.

According to the Individuals Right Under HIPAA to Access their Health Information, it says:

> *The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. See 45 CFR 164.514(h). The Rule does not mandate any particular form of verification (such as obtaining a copy of a driver's license), but rather generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided the verification processes and measures do not create barriers to or unreasonably delay the individual from obtaining access to her PHI, as described below. Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the individual is requesting and/or receiving access – whether in person, by phone (if permitted by the covered entity), by faxing or e-mailing the request on the covered entity's supplied form, by secure web portal, or by other means.*

Therefore, the CARIN Alliance supports open standards for providers, EMR systems and applications to follow when ID proofing someone across systems who may be coming through a third-party application. While we believe in the short-term, users may continue to be ID proofed via provider portals, we believe in the long-term there will and should be ways to perform ID proofing that are consistent with NIST and other relevant standards. We anticipate development in other industries, and in healthcare, of federated, decentralized identity-proofing and authentication services, which can streamline the process for requesting electronic health information across the ecosystem.

RECOMMENDATION TO ONC: The CARIN Alliance recommends the ONC support the NIST Special Publication 800-63A, "Digital Identity Guidelines: Enrollment and Identity Proofing Requirements" and implement Identity Assurance Level 2 (IAL2) for a consumer who is using a third-party application to request electronic access to their health information and allows for both remote and in-person ID proofing.

2. The ability to **ID proof** who is requesting access to the consumer's digital health information

RECOMMENDATION TO ONC: The CARIN Alliance recommends the ONC support the NIST Special Publication 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management" and implement Authenticator Assurance Level 1 (AAL1) for a consumer who is using a third-party application to request electronic access to their health information.

3. The ability to **select the application(s)** the consumer would like to send their digital health information

4. If applicable, the **caregiver(s)** or **authorized representatives** who should receive access to the consumer's digital health information with consumer authorization.

5. The **frequency and length of time** the consumer and their authorized caregiver will permit the EMR to provide access to their digital health information to the third-party application or data store of the consumer's choice.

6. The **types of data** authorized to be shared, where feasible and as supported by standards, especially with respect to sharing potentially sensitive data

The CARIN Alliance is currently working on the details to build these consent requests digitally and looks forward to working with the ONC on this important topic.

Use Case 2: The process for how a provider / EMR sends the electronic health information via APIs to a third-party application or data store of the consumer's choosing

This use case is focused on the technology side of consumer-directed exchange. We are striving to develop a preferred technology workflow that will share how information can be sent securely and electronically so that consumers are able to receive their information in the manner of their choosing.

We believe there are a few key technology open standards that should be promoted by the industry and the ONC to effectively transmit information between EHRs and a consumer's third-party application.

Argonaut Data Query Implementation Guide
The CARIN Alliance promotes and supports the use of HL7's FHIR DSTU2 APIs and the Argonaut Data Query Implementation Guide which includes the use of the SMART on FHIR authorization guide.

OAuth 2.0 Dynamic Client Registration Protocol
Currently, the method for registering an application with an EHR vendor to simply provide the ability for the application to act on behalf of a consumer involves each application going to individual EHR application stores

to receive an access token. This process is cumbersome and costly for both the application and the EHR vendor.

The CARIN Alliance believes using the OAuth 2.0 Dynamic Client Registration Protocol will streamline the process for receiving an access token, allows patients to use *any* application of their choice, and reduces overall administrative cost.

Refresh Tokens

Currently, there is not a consensus approach for how refresh tokens are managed or selected by the consumer. The CARIN Alliance believes the consumer should have the ability to choose the frequency and length of time the application has to access information on their behalf. This should be a user-controlled and user-governed choice that is made through the application of the user's choice.

Application Endorsements

Applications need to have a way to ensure third-party application endorsement of health care applications. POET was conceived as a means to represent third-party application endorsement for health care applications. POET's goal is to help consumers distinguish between applications that have an endorsement versus applications that have no pedigree (i.e., are untrusted and could be malicious).

The CARIN Alliance supports open standard approaches to third-party application endorsements such as POET and believes it's an important advance in providing consumers access to their health information.

Public availability of the FHIR endpoints

For health IT applications to readily access consumer data across multiple systems, it's important for the FHIR endpoints to be publicly available. Therefore, the CARIN Alliance supports storing and maintaining the FHIR endpoints with a trusted third-party (registry.fhir.org, NATE, etc.) or within the ONC.

V. PRIVACY AND SECURITY

The CARIN Alliance supports use of effective, and appropriate voluntary privacy and security practices, and in full and transparent disclosure of these practices to consumers in forms consumers can easily understand. We believe the ONC's 2016 Model Privacy Notice is an valuable resource for applications to use to develop appropriate privacy and security practices, and to provide consumers with the information they need to understand how their data is being used, stored, and transmitted. We also believe there is an opportunity to make enhancements to the MPN by doing the following:

- Simplify the form to focus on major topics and a description rather than configurable parameters which may change over time. The 12 CARIN trust framework principles listed above could provide additional guidance on how the MPN might be updated in the future.
- The section on 'How this technology accesses other data' is largely duplicative to the setting on most phones. Trying to keep up with how phone settings change over time will become difficult.
- Identify which areas of the FTC's financial services model privacy notice can be reused

Within an application's terms of service, the following list provides a sample set of considerations that may be used when developing a terms of service template in addition to the model privacy notice. Most likely,

applications will have both a privacy notice and terms of service. We believe these terms should be developed with a more user-friendly voice that is understandable (i.e., eighth-grade reading level).

Sample consumer terms of service

- User Acceptance of Terms of Use
- Description of Limited Use and Availability
- Agree to a Patient Agreement and Consent ("Patient Consent")
- Duty of Consumer to Provide Information, Access, and Connectivity
- User Accounts and Security
- Ownership of Information Submitted to the application
- Acknowledgement of Highly Confidential Information
- Prohibited Use
- Right to Monitor
- Third Party Goods and Services
- Termination
- Disclaimers
- Indemnification
- Notices
- Electronic Communications
- Governing Law
- No Agency Relationship
- Assignment
- Third Party Beneficiaries

VI. ONC COMMENT AREAS

The principles and details provided above guide our comments for each of the ONC comment areas.

a. Standardization

We recommend that the trust framework guidelines "recommend" that non-covered entities providing applications adhere to relevant industry and federally recognized technical standards, policies, best practices, and procedures, but not in ways which might limit ability to innovate in ways that can lead to improvements in access to data for consumers and their designees. We recommend the use of endorsements and certifications to communicate an application's ability to adhere to relevant standards, policies, best practices and procedures. We recommend that these be made broadly available to the industry and consumers through open services.

b. Transparency

We recommend that the methods by which exchange occurs between covered entities and non-covered entities be open and transparent. We support the idea of multiple exchange networks co-existing, and competing, to add value to applications, consumers and covered entities, as long as they use trust frameworks in alignment with these principles. We support open, transparent governance for any of these networks.

c. Cooperation and non-discrimination

We strongly support implementation of health information sharing networks that support exchange among stakeholders across the continuum of care, as well as with non-traditional stakeholders and consumers. We support inclusion of new classes of non-traditional actors engaged in accessing and sharing health data with

applications, such as community health organizations, social services groups, consumer-groups, social network platforms, precision-medicine researchers, genomics labs, application companies, internet of health things providers, A.I. technology companies and developers, and other non-traditional health data sources and users. Such collaboration should formally include support for exchange among competing parties.

d. Security and patient safety

We support exchange of electronic health information in a safe, secure way, as set forth in our principles. Consumers should have the unrestrained right to have their data shared with any application they choose – including an insecure application, with poor data integrity, that does not promote patient safety. However, we strongly support the use of a system of endorsements and certifications that can make it simple and easy for consumers to understand the level of capabilities of applications they choose, and make application choices they feel are best for them.

e. Access

We strongly support the principle that consumers and all who serve them should have easy access to their comprehensive, machine-readable electronic health information when, where and how they want it. We recommend that specific comments be made about what it means to provide easy access to data for consumers and their applications.

f. Data-driven choice

As noted above, we strongly support ability to exchange multiple records at one time with consumer-authorized applications. Ability for consumers to request their right of access to one or many locations, through an application, is user friendly and technically feasible. Asking consumers to sign customized individual right of access forms for each system they seek to connect, or requiring consumers to physically sign such forms, would be a huge barrier for applications and consumers, while also being a costly burden for covered entities supporting that workflow.