February 20, 2018

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 USCDI Public Comments

Dear Dr. Rucker:

On behalf of the CARIN Alliance, we want to thank you for the opportunity to comment on the Office of National Coordinator's (ONC's) draft Trusted Exchange Framework (TEF) and United States Core Data for Interoperability (USCDI) in conjunction with the 21st Century Cures Act.

As you are aware, the CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers, individuals, and caregivers. We are committed to enabling consumers and their authorized caregivers 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 made available under the 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 have centered our comments around the following general themes:

- ONC should provide the capability for an app selected by an individual to be able to easily, and without charge, query/pull information for Individual Access from QHINs, Participants and other End Users without requiring that app to make information available to other Participants and End Users for all of the Permitted Purposes except where the individual has provided consent consistent with the app's terms of use.

- ONC should consider changing wording in the document from "patient" to "individual" or "consumer." Patient implies only those individuals who have interacted with the health system while "individuals" or "consumers" imply anyone who may or may not have had a recent acute care event. In the future, health information that flows between CEs and NCEs will involve all types of health care and non-health care data (i.e., SDOH), including those who have recently engaged the health care system and those who have not.

- In addition, we strongly encourage the ONC to include a more detailed definition of what would be considered "individual access" so the ONC, OCR, and the industry can better define the difference between a HIPAA authorization and individual access. Here is some language to consider:

  A request for individual access to their ePHI must be processed if it:

- Is submitted directly by a consumer-controlled end user (CCEU and defined below) that meets the identity proofing and authentication requirements of the CA;
- Clearly indicates the destination for sending information per the CA; and
- Is requesting data from the then-current USCDI.

No Participants, End Users or Qualified HINs may require the submission of a HIPAA authorization (as defined in 45 CFR 164.508) or a business associate agreement in order to process an individual access query/pull from an app that has been engaged by, and works on behalf of, an individual.

Thank you again for considering our comments and recommendations.

David Lee
Leavitt Partners
On behalf of the CARIN Alliance

I. Individual right of access vs. HIPAA authorization requests

The CARIN Alliance comments are exclusively focused on how the TEF and CA affects an individual's right and ability to access their health information in as seamless, secure, and as streamlined way as possible. We will not focus our comments on any aspects of the TEF and CA that involve exchange between HINs, QHINs, or two or more covered entities for the other Permitted Purposes. Our comments focus on how data can be electronically exchanged between a covered entity (or business associate) and a non-covered entity (e.g., consumer, community-based organization, third-party application) when the consumer requests their information using their individual right of access right provided to them under HIPAA.

There are two very distinct types of electronic health information exchange requests that involve an individual. One is where individuals sign a **HIPAA authorization** to legally allow a covered entity to share information with another entity (such as for benefits determination, one of the Permitted Purposes). The other type of request is when an individual invokes their **right of access** under HIPAA and requests a covered entity to share their information with a non-covered entity which could include a third-party application, community-based organization (CBO), or personal use access. Once an individual receives access to their health information, they can direct that information to anyone or any application they wish with no restrictions or paperwork (e.g., DURSA, business associate agreements, etc.) involved in the exchange of information. Both a HIPAA authorization and right of access request are **separate and distinct** ways in which an individual is involved in the transfer of their health information. The permitted purpose of "individual access," when exercised by an individual (or a personal representative, per HIPAA), should be considered to be a request for information pursuant to the individual's right of access under 45 CFR 164.524 and should **not** require the execution of a HIPAA authorization. In addition, when an individual invokes their right of access that request should extend through the entire system after the QHIN executes its broadcast query. Finally, it's important to understand this individual right of access request extends to any covered entity whether it is a provider, health plan, or health care clearinghouse.

CARIN Comments: The CARIN Alliance would strongly recommend that ONC reexamine the TEF and CA and clearly indicate the differences between when an individual is making a HIPAA authorization request versus a right of access request.

On its website, the Office of Civil Rights has distinguished between a HIPAA authorization request and a right of access request as follows:

HIPAA Authorization	Right of Access
Permits, but does not require, a covered entity to disclose PHI	**Requires** a covered entity to disclose PHI, except where an exception applies
Requires a number of elements and statements, which include a description of who is authorized to make the disclosure and receive the PHI, a specific and meaningful description of the PHI, a description of the purpose of the disclosure, an expiration date or event, signature of the individual authorizing the use or disclosure of her own PHI and the date, information concerning the individual's right to revoke the authorization, and information about the ability or	Must be in writing, signed by the individual, and clearly identify the designated person and where to the send the PHI

HIPAA Authorization	Right of Access
inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.	
No timeliness requirement for disclosing the PHI Reasonable safeguards apply (e.g., PHI must be sent securely)	Covered entity must act on request no later than 30 days after the request is received
Reasonable safeguards apply (e.g., PHI must be sent securely)	Reasonable safeguards apply, including a requirement to send securely; however, individual can request transmission by unsecure medium
No limitations on fees that may be charged to the person requesting the PHI; however, if the disclosure constitutes a sale of PHI, the authorization must disclose the fact of remuneration	Fees limited as provided in 45 CFR 164.524(c)(4)

II. TEF Introduction

TEF LANGUAGE: The vision we seek to achieve is a system where individuals are at the center of their care and where providers have the ability to securely access and use health information from different sources. A system where an individual's health information is not limited to what is stored in electronic health records (EHRs) but includes information from many different sources (including technologies that individuals use every day) and provides a longitudinal picture of their health.

CARIN COMMENTS: The CARIN Alliance completely agrees with the ONC's vision to ensure individuals are at the center of their care. We believe individuals have a right to access their data from any provider in the country which includes the ability to access individual data "without special effort, using application programming interfaces" as stated in the 21st Century Cures Act.

We also believe these same application programming interfaces (APIs) should be used to enable the individual to compile / construct their complete longitudinal health record in an open standard format and their right to direct health information exchange.

TEF LANGUAGE: In an effort to develop and support a trusted exchange framework for trusted policies and practices and for a common agreement for the exchange between HINs, the proposed Trusted Exchange Framework supports four important outcomes: 1) providers can access health information about their patients, regardless of where the patient received care; 2) patients can access their health information electronically without any special effort; 3) providers and payer organizations accountable for managing benefits and the health of populations can receive necessary and appropriate information on a group of individuals without having to access one record at a time (Population Level Data), which would allow them to analyze population health trends, outcomes, and costs; identify at-risk populations; and track progress on quality improvement initiatives; and 4) the health IT community has open and accessible application programming interfaces (APIs) to encourage entrepreneurial, user-focused innovation to make health information more accessible and to improve electronic

health record (EHR) usability. All four of these outcomes shall be accomplished in compliance with applicable HIPAA Rules' requirements.

CARIN COMMENTS: The CARIN Alliance wholeheartedly agrees with this section of the document. We also believe "without any special effort" and "open APIs" should be defined as the ability for the individual to access their electronic health information on demand, in real-time, and at no cost as indicated in 5.3.2 of the common agreement. Wherever possible, we would also recommend the trusted exchange framework use the term "individual" rather than "patient." In the future, individuals will access their health data whether or not they have had a recent encounter with the health care system.

TEF LANGUAGE: ONC intends to select through a competitive process a single RCE that will incorporate the Part B requirements into a single common agreement to which Qualified HINs may voluntarily agree to abide. The RCE will be tasked with operationalizing the Trusted Exchange Framework. We believe that a single, industry-based RCE is best positioned to operationalize the Trusted Exchange Framework. Implementing the TEF requires day-to-day management and oversight of unaffiliated Qualified HINs, including: onboarding organizations to the final TEF, ensuring Qualified HINs comply with the terms and conditions of the TEF, addressing non-conformities with Qualified HINs, developing additional use cases, updating the TEF over time, and working collaboratively with stakeholders. ONC intends to work closely with the RCE and to be continually involved in implementation of the TEF. We look forward to stakeholder comment on this approach.

CARIN COMMENTS: The CARIN Alliance looks forward to further clarification from the ONC on what the RCE is and what its unique role will be in the health care interoperability ecosystem. We also seek to better understand what impact the RCE may have on providing individuals access to their health information. Based on the description above and other language in the document (especially Part B), we believe the ONC intends for the RCE to play a number of different roles including: convener, arbitrator, contracts administrator, trainer, enforcer, overseer, and the SDO/technical compliance entity. While these roles may be needed to administer and oversee the trust framework, the CARIN Alliance is not aware of any one organization in the market today who possesses all of these attributes.

As such, we would recommend the ONC specify the unique roles required of the RCE and allow one organization to be the RCE but encourage the RCE to develop a structure so a "board of advisors" could meet regularly under the RCE's direction to provide them input based on their specific areas of expertise. For example, a single RCE could have a "board of advisor"' that would include representation (if the RCE didn't possess these attributes already) from the standards community, implementation community, individual/caregiver community, non-covered entity community, public health community, venture capital / innovation community, and legal/trust framework community.

III. TEF Comment Process

TEF LANGUAGE: Are there standards or technical requirements that ONC should specify for identity proofing and authentication, particularly of individuals?

CARIN COMMENTS: Individuals do not currently have a seamless method to request access to PHI across different EMRs without logging in to each portal separately. We are supportive of the SMART on FHIR workflow that allows the user to enter a pre-registered portal user name and password to access their health information using a third-party application. When an individual has their data spread across multiple portals (including some that may be unknown to the individual) there is no easy way to aggregate all of their data without remembering every provider the individual has ever seen, registering with all of those portals, and then remembering every single username and password so they can be used in the application. That is not a good user experience.

The CARIN Alliance would suggest unifying identity proofing and authentication through the utilization of shared login services that conform to NIST 800-63 standards. For example, the Department of Veterans Affairs has implemented a unified authentication approach aligned to NIST 800-63 standards at www.Vets.gov. Implementing this type of an approach across the entire commercial provider community will enable veterans to access Community Choice Care Act providers with the same ID proofing credential they used for Vets.gov. This can be done remotely following the NIST standards or in person. Similarly, if a veteran were to initially create a certified IAL2 credential with a Community Choice Care Act provider, that credential could also be accepted by www.Vets.gov.

A NIST certified shared login service need not replace a provider or EMR's direct credentialing flows but should act as a universally recognized login option in addition to the proprietary login flows similar to how Facebook and Google provide fast login routes on websites operating at low levels of trust as an option to avoid creating a login and password directly with the site. NIST IAL2 and AAL2 credentials would be recognized as a common, trusted login for cross-entity authentication to PHI. Individuals may request access from multiple EMRs and providers with the same authority through a single-credentialing and authentication event without having to login to each provider or EMR individually.

NIST 800-63 standards provide the foundation for interoperability between organizations at a given level of risk the same way Visa's standards provide trust between card issuing banks and merchants. Authentication interoperability for shared login services should use open standards such as OAuth 2.0, OpenID Connect, and SAML 2.0 to transmit identity attributes.

All certified identity providers would be published on a publicly-available government website (https://www.idmanagement.gov/trust-services/#consumer-identity-credentials) to provide transparency with everyone in the health care ecosystem. Based on initial conversations with major health delivery systems and health IT companies, the CARIN Alliance believes if ONC creates or helps facilitate the creation of an environment where key stakeholders (e.g.., hospitals, EHR vendors, Health IT companies, etc.) can become a certified credentialing authority at an IAL2 level and ensures EHR vendors can accept that IAL2 certified credential from anyone who is a certified ID provider, the market will develop a proliferation of entities who develop unique business models to compete for the opportunity to credential an individual.

Part A– Principles for Trusted Exchange

Principle 2 - Transparency: Conduct all exchange openly and transparently.

C. Publish, keep current, and make publicly available the Qualified HIN's privacy practices.

TEF LANGUAGE:

1. Qualified HINs must comply with all Applicable Laws regarding the use and disclosure of ePHI or other Electronic Health Information.
2. Clearly specify the minimum set of "permitted purposes" for using or disclosing ePHI or other identifiable Electronic Health Information within the TEF and promote limiting the use of identifiable Electronic Health Information to the minimum amount required for non-treatment purposes. If there are technical variables, the Qualified HINs should clearly specify them.
3. Qualified HINs must have the capability to document and/or capture patient consent or written authorization if required by law and communicate such consent upon request.
4. Qualified HINs must not impede the ability of patients to access and direct their own Electronic Health Information to designated third parties as required by HIPAA.
5. Qualified HINs must have policies and procedures to allow a patient to withdrawal or revoke his or her participation in the exchange of his or her Electronic Health Information on a prospective basis.

CARIN COMMENTS: The CARIN Alliance believes in #3 ONC should differentiate between a patient authorization and an individual right of access request permitted purpose. Specifically, ONC should be clear that this represents the legal requirements for HIPAA consent or authorization (such as a HIPAA authorization, where one is required, or consent or authorization requirements in 42 C.F.R. Part 2 or state law). What should be required for individuals to exercise their HIPAA individual right of access is not "consent" or "authorization" but proof that the request is coming from the individual or a personal representative, which can be done by requiring IAL2 and AAL2 certification. We strongly support #4. We also note that QHINs, who will be business associates under HIPAA, are expressly authorized by HITECH (Section 13405(e)(2), as added by Section 4006(b) of the 21st Century Cures Act) to provide individuals or their designees with access to, or a copy of, their protected health information ("if the individual makes a request to a business associate for access to, or a copy of, [PHI] about the individual, or if the individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy…or grant or transmit such access or copy to such person or entity designated by the individual…" (emphasis added). For #2, the CARIN Alliance seeks clarification from ONC on how each permitted purpose needs to be verified electronically.

Additionally, End Users should have access only to the information they need for a given purpose, consistent with the HIPAA Privacy Rule's minimum necessary standard. We agree that reducing the friction of accessing medical information at the individual or population health level is an important goal; however, we have concerns with the potential pitfalls of stakeholders having unprecedented access to information across the health care system. Current data request processes, while limiting, are narrowly scoped for specific use cases and involve some level of "gating" that helps prevent abuse and helps enforce compliance with minimum necessary standard on both ends of the transaction (collection (query) and disclosure). Automating and increasing the volume of data access, without some mechanisms in place to help enforce minimum necessary at both ends, may invite misuse. We strongly recommend that ONC consider all ramifications of bulk data access, including an individual's privacy and security of their information, and situations that inadvertently result in "select all & copy." Clearly, increasing ease of access to data is an imperative; however, ONC must also consider the need to hold entities accountable,

including assuring that covered entity End Users can comply with their minimum necessary obligations in both launching and responding to queries. We recommend ONC explore mechanisms such as 1) requiring QHINs to monitor query and response logs and take action against Participants and End Users who abuse the openness of the system through overly broad queries (for example, suspending or revoking query rights) and 2) establishing a mechanism for receiving and promptly resolving complaints about abuse of the system.

TEF LANGUAGE: The draft Trusted Exchange Framework requires a Qualified HIN that is not a Covered Entity to publish and make available a notice as well.

CARIN COMMENTS: Transparency regarding what personal information is collected, and for what purposes that information is accessed, used, and disclosed, is a hallmark of fair information practices, which are the foundational principles underlying privacy law. QHINs are business associates under HIPAA, and as such, are not required to publish a HIPAA Notice of Privacy Practices unless the QHIN is a covered entity. In addition, such notice often does not describe actual information practices. Because the TEF anticipates that QHINs may collect and share information for purposes beyond the permitted purposes, it is important that information on a QHIN's data practices be available to the public.

> **Principle 5 - Access: Ensure that Individuals and their authorized caregivers have easy access to their Electronic Health Information.**
>
> **A. Do not impede or put in place any unnecessary barriers to the ability of patients to access and direct their Electronic Health Information to designated third parties.**

TEF LANGUAGE: Stakeholders who maintain Electronic Health Information should (1) enable individuals to easily and conveniently access their Electronic Health Information, (2) be able to direct it to any desired location, and (3) ensure that individuals have a way to learn how their information is shared and used. This principle is consistent with the HIPAA Privacy Rule, which requires Covered Entities to provide PHI to individuals in the form and format in which they request it, if it is readily producible in that form and format. This means that if it is stored electronically, individuals can request it and access it electronically.

CARIN COMMENTS: We strongly agree. If the data can be accessed via APIs, individuals can request it be sent via an API to a third-party application of the individual's choosing. Since the data is "readily producible" electronically with "no special effort," the data should be sent to the individual at no charge as outlined in Section 5.3.2 of the common agreement.

TEF LANGUAGE: HIPAA also requires Covered Entities and Business Associates to send PHI to a third party of the patient or authorized representative's choosing, upon request.

CARIN COMMENTS: We strongly agree. This concept should be emphasized throughout the document. ONC should also emphasize that individual access requests do not require presentation of documentation that a consent or authorization has been executed. We would also recommend defining what is meant by a third party. The CARIN Alliance believes a third party could be any covered entity or non-covered entity of the individual's or authorized representative's choosing. This would enable individuals to have their information transmitted to other providers, under their individual right of access, thereby allowing individuals to send their information to any third party of their choosing without going through a covered entity's HIPAA release process, which is often burdensome, untimely, and unreliable.

TEF LANGUAGE: Covered Entities and Business Associates may not impose limitations through internal policies and procedures that unduly burden the patient's right to get a copy or to direct a copy of their health information to a third party of their choosing.

CARIN COMMENTS: We agree. This language should also include an individual's personal representative or caregiver. For purposes of this letter, the term "caregiver" must at least include 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.

TEF LANGUAGE: Likewise, Qualified HINs and their participants – most of whom are Covered Entities or Business Associates – should not limit third-party applications from accessing individuals' Electronic Health Information via an API when the application complies with Trusted Exchange Framework requirements and is directed by the individual.

CARIN COMMENTS: We strongly agree. This should include all qualified HINs including HIEs. However, as we have discussed in other areas of our response, an individual's data may be limited to what is reasonable and necessary – meaning that the query could involve all or only some of the individual's data depending on the specific use case(s) being invoked.

TEF LANGUAGE: In addition, Qualified HINs and their Participants should commit to training all staff members on helping individuals obtain electronic access as demonstrated by ONC's access videos and infographic.

CARIN COMMENTS: We strongly agree. Participants and Qualified HINs should also educate their staff members on why providing individuals access to their health information is required under HIPAA.

TEF LANGUAGE: Much like individuals' access to their health information as required by HIPAA is important, it also is important for individuals to have access to information about who else has accessed or used their health information. As the Fair Information Practice Principles (FIPPs) of the Nationwide Privacy and Security Framework on openness and transparency states, "[p]ersons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format." HINs should commit to following this principle, and should provide such opportunities electronically whenever possible, particularly when an individual makes the request electronically. NPP can also serve to help individuals understand how and when their health information is shared.

CARIN COMMENTS: We strongly agree. We appreciate the ONC's acknowledgement of many of the 12 CARIN Alliance Trust Framework principles in the draft TEF. We believe there is an opportunity to develop even more specificity around the following principles:

- **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.

  Additional work is needed by private industry and the ONC to accurately and effectively federate a consumer's individual right of access privileges throughout the health care ecosystem. The CARIN Alliance plans to work on this topic in 2018. We would appreciate hearing more about how ONC plans to address this issue in later versions of the TEF.

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

  It's important to note the "entire health record" includes health plan and claims data. As a covered entity, health plans are under the same obligation as providers to exchange data with individuals. The CARIN Alliance is also examining ways health plans can more effectively exchange data across multiple systems with consumes. We would welcome the opportunity to work with the ONC to examine how the TEF might evolve to accommodate the ability for a health plan to share information with consumers across systems.

B. Have policies and procedures in place to allow a patient to withdraw or revoke his or her participation in the Qualified HIN.

TEF LANGUAGE: Some individuals may prefer not to have their health information electronically shared via a Qualified HIN. Consequently, Qualified HINs and/or their participants must maintain policies and procedures that allow a patient to revoke his/her participation in the Qualified HIN on a prospective basis. Such policies and procedures must be easily and publicly available and be consistent with the HIPAA Privacy Rule right of an individual to request restriction of uses and disclosures, and the process for revoking participation must be easily accomplished by patients.

CARIN COMMENTS: We appreciate providing individuals with the opportunity to opt out of having their EHI shared through QHINs but individuals should be able to opt out of providing information but still retain their right to exercise their individual right of access to obtain/pull information via the application of their choice.

Principle 6 - Data-driven Accountability: Exchange multiple records for a cohort of patients at one time in accordance with Applicable Law to enable identification and trending of data to lower the cost of care and improve the health of the population.

A. Enable participants to request and receive multiple patient records, based on a patient panel, at one time.

TEF LANGUAGE: Additionally, caregivers who are authorized legal representatives, known as "personal representatives" under HIPAA, may wish to access all of their family's records at one time, rather than having to request one record at a time for each family member to the extent permitted by law.

CARIN COMMENTS: We strongly agree. We suggest the ONC includes a requirement that each personal representative is uniquely ID proofed to IAL2 so they can be connected with the individual electronically. This will allow the personal representatives to access the data on behalf of the individual. Accessed information should include an audit trail of which personal representatives accessed the information, what information was access, and when the information was accessed. Additionally, individuals designated as caregivers, in addition to personal representatives, should be able to access information on the individual's behalf.

We believe the term "caregiver" needs to be defined. Senator Booker's In-Home CARE Act (S. 2866) may provide a starting point for further discussion. It states:

> "The term 'caregiver' means 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."

We recommend that ONC first includes both caregivers and personal representatives as part of the TEF language and then engages with industry to help better define an actual caregiver.

Part B – Minimum Required Terms and Conditions for Trusted Exchange

General Comments

The CARIN Alliance would recommend the ONC consider including removing the specific technical standards information from the common agreement and including it in a separate implementation guide that includes what standards would be required for what use case. This will continue to ensure the ONC can measure the industry based on the adoption of agreed upon standards but as the standards change, the implementation guide will get updated rather than the entire common agreement. The implementation guide will still be required as part of the common agreement and will be updated and overseen by the RCE, "board of advisors", standards bodies, and the ONC.

When an individual invokes his or her individual right of access through a third-party application, the individual should not be concerned who is the majority or minority owner of the application. As such, the CARIN Alliance would recommend the ONC consider including language in the common agreement that says when an individual invokes this or her individual right of access, the request should be granted by everyone in the data sharing ecosystem (must share not may share) regardless of who owns the application itself so long as the individual makes a right of access request. For example, an application which is minority or majority owned by a covered entity when acting on behalf of the individual should be treated similarly (must share not may share) to when an application which is owned by a venture capital or private equity firm. Doing otherwise would create an unfair advantage in the market place.

TEF Language:

2.1 No Limitations on EHI Aggregation. A Qualified HIN shall not limit the aggregation of EHI that is exchanged among Participants, provided that any such EHI aggregation is in support of the permitted purposes and in accordance with all Applicable Law.

CARIN Comments:

We would recommend there are no limitations on EHI Aggregation when an individual or their authorized caregiver makes an "individual right of access" request to QHIN.

TEF Language:

3.1.2 As more fully described in the following provisions of this Section 3, the Qualified HIN's Broker shall send and receive all of the "patient matching data" so labelled and specified in the 2015 Edition certification criterion set forth at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable standards adopted in the future by HHS) when and to the extent that such data is electronically available within or through the Qualified HIN's network to the extent permitted under Applicable Law.

CARIN Comments:

In addition to the "patient matching data" found in the 2015 Edition certification criteria and to remain consistent with the rest of the common agreement, we would recommend the QHINs be required to send a phone number and an email to identify a unique individual across systems. Without this information, it will be extremely difficult to identify individuals across systems.

TEF Language:

3.3 Patient Demographic Data for Matching

3.3.1 Each Qualified HIN shall support the exchange of the patient matching data enumerated in the 2015 Edition certification criterion adopted at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable certification criteria adopted in the future by HHS) to the extent permitted by Applicable Law.
3.3.2 Participants who collect and maintain the patient matching data enumerated in the 2015 Edition Certification Criterion adopted at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable certification criteria adopted in the future by HHS) shall provide all such data to the extent permitted by Applicable Law when initiating or responding to Queries/Pulls.

CARIN Comments:
In addition to the "patient matching data" found in the 2015 Edition certification criteria and to remain consistent with the rest of the common agreement, we would also recommend the QHINs be required to send all of the required user proofing and authentication information necessary to identify a unique individual across systems. Without this information, it will be extremely difficult to identify individuals across systems.

TEF Language:

5.2.2 Non-Discrimination. This provision permits a QHIN to treat another QHIN, or a Participant or End User, "differently based on a reasonable and good faith belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the CA (including compliance with Applicable Law) in any material respect. "

CARIN Comments:
We have concerns with this provision because it puts entities with health information that individuals have a right to access in a position to decline to honor an individual's access request on the basis that the recipient (such as an application) selected by the individual has unreasonable or insufficient (in the views of the entity) privacy and security practices. HIPAA, as amended by the HITECH Act, gave individuals the ability to have their health information sent to the person or entity of their choice, without the caveat that this third party be compliant with HIPAA or any other minimum privacy and security practices. It is already the case that neither a HIPAA covered entity or a business associate is legally responsible for privacy and security practices of downstream recipients of PHI, as long as the disclosure of the information is HIPAA-compliant.

TEF Language:

5.3.2 Fees. This provision states that QHINs may not charge any amount for responding to Queries/Pulls for the Permitted Purposes of Individual Access, Public Health or benefits determination.

CARIN Comments:
We strongly support the prohibition on fees for queries/pulls for individual access.

TEF Language:

6.1.1 Individual Access**.** Each Qualified HIN agrees and acknowledges that individuals have a right to access, share and receive their available ePHI in accordance with the HIPAA Rules, section 4006(b) of the 21st Century Cures Act, and the terms and conditions of the Common Agreement. Each Qualified HIN agrees and acknowledges that individuals have a right to direct a HIPAA Covered Entity to transmit a copy of ePHI in a designated record set to any third parties designated by the individual in accordance with Applicable Law. Similarly, each Qualified HIN agrees and acknowledges that individuals have a right to direct a Participant or End User to transmit a copy of EHI to any third parties designated by the individual in accordance with Applicable Law.

CARIN Comments:

We would support this language. In Part B of the TEF, it defines individual access as the right of individuals to access and obtain a copy of ePHI pursuant to applicable law, including HIPAA. However, in that individual access definition (page 27 of the TEF), it notes that with respect to an individual access query, the response must be provided, whether that query is submitted by an individual or an app selected by an individual. Furthermore, that app must comply with all the appropriate privacy and security requirements of this agreement **(and applicable law) and be connected to, or itself be, a Participant or End User.**

It may not be possible for some third-party applications to be a Participant or an End User under the terms and conditions in Part B of the TEF, because the TEF, in Sections 9.1.1 and 10.1.1 requires Participants and End Users respectively to "support all of the Permitted Purposes by providing all of the data classes [of] the then current USCDI when and to the extent available when requested and permitted by Applicable Law." It also obligates both to "respond to Queries/Pulls for the Permitted Purposes." (Section 9.1.1 for Participants and Section 10.1.1 for End Users). Participants and End Users also are not permitted to "discriminate" by not exchanging with certain other entities or individuals.

As an example, consumer-controlled apps frequently make commitments to their customers that they will only disclose an individual's health information with the individual, because the individual will control their own record. That app could not execute the common agreement (CA) or participate with a QHIN who has committed to the terms of the CA, because the CA requires Participants and End Users to release an individual's EHI (without regard to whether or not the individual consented). Specifically, refusing to share for all of the Permitted Purposes, or with particular persons or entities, would potentially violate Sections 9.1.1 and 10.1.1, as well as the nondiscrimination provisions in Sections 9.1.2 and 10.1.2 of Part B in the TEF.

The CARIN Alliance believes that with respect to consumer-controlled tools, the availability of EHI for any of the Permitted Purposes should depend on the agreement or consent of the consumer to release the information. The language in the CA definition of "individual access" contemplates that consumer-controlled apps would not have to necessarily be Participants or End Users but could instead "connect to" a Participant or End User. However, the entire structure of the TEF and CA does not describe how an entity "connects" into the framework without being at least an End User. If individuals (or apps acting on their behalf) are to fully realize the promise of the TEF and CA (and exercise of their HIPAA rights via the TEF and CA), there needs to be a clear way for individuals to connect into the infrastructure, but without giving up their rights to control how information in a personal app is further disclosed.

One possible solution is to create a separate category of End User for consumers (as well as personal representatives and other caregivers acting on behalf of the consumer) and their apps. The "Consumer-Controlled End User" (CCEU, a term coined for purposes of this discussion) should not be required to provide data in response to all queries; however, they must be able to connect into the infrastructure (presumably through a Participant) in order to query data for consumers, where the individual (or their legal representative) makes and controls the requests exercising their HIPAA rights of individual access (potentially the only permissible purpose for which they can submit queries). Access by any other participant in the TEF would not constitute the permitted purpose of individual use.

To assure clarity on which entities are – and are not – consumer-controlled, we suggest leveraging the definition of personal health record from the HITECH Act, which says in part the term "personal health record" means an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. This is distinct from an "electronic health record," which is information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. The HITECH Act also made clear that such

personal health records would only be "HIPAA business associates" in circumstances where a personal health record is offered to individuals "as part of" an electronic health record" (see Section 13408 of the HITECH Act).

If the ONC proceeds in making this change, the TEF and, subsequently, the CA will need to adjust the Participant responsibilities accordingly, so they are not held responsible for requiring CCEUs to meet all of the same terms and conditions of other End Users. For example, the breach notification obligations should be those imposed on personal health records by the HITECH Act (pursuant to Section 13407). Also, although we agree with requiring CCEUs to meet minimum standards for identity, it's not clear why CCEUs should be required to meet other privacy and security safeguards, as individuals have a choice of where to send their information, even if the choice is a poor one from a privacy and security standpoint). The FTC remains authorized to enforce its privacy and security expectations on CCEUs consistent with its FTCA authority.

Another option for assuring that individuals are able to access information through the TEF ecosystem using consumer-controlled apps is to define the concept of "availability." Specifically, Participants and End Users are required to disclose EHI for the Permitted Purposes to the extent it is "available." For consumer-controlled apps, the "availability" means the consumer has agreed to make the information available to the particular querying person or entity for the particular purpose. However, we could foresee a circumstance where End Users seeking to minimize their obligations to share information might voluntarily adopt consent requirements. Consequently, if the individual had not specifically consented to sharing information in a particular circumstance, the information would not be "available." To avoid such an outcome, we suggest by creating a specific class of End User for consumer-controlled apps, borrowing from the HITECH Act definitions in order to help differentiate between apps that are "personal health records" versus those that are business associates subject to HIPAA.

To assure that questions about legal liability do not disrupt the ability for individuals (or their personal representatives or caregivers) to exercise their right of individual access using the TEF ecosystem, we suggest OCR and FTC issue guidance on their respective breach reporting regulations pursuant to the HITECH Act, so that covered entities and business associates are clear about their HIPAA breach notification obligations in circumstances where a breach occurs after information is disclosed, at the request of a consumer, to a consumer-controlled app (or "personal health record") via an API and the vendors of these apps are aware of their breach notification obligations to the FTC under the HITECH Act. Such clarity will provide greater legal certainty to entities seeking to facilitate data sharing with consumers via apps and will assure that individuals are notified by the appropriate entity in the event a breach occurs.

In addition, we strongly encourage the ONC to include a more detailed definition of what would be considered "individual access" so the ONC, OCR, and the industry can better define the difference between a HIPAA authorization and individual access. Here is some language to consider:

A request for individual access to their ePHI must be processed if it:

- Is submitted directly by a CCEU that meets the identity proofing and authentication requirements of the CA;
- Clearly indicates the destination for sending information per the CA; and
- Is requesting data from the then-current USCDI.

No Participants, End Users or Qualified HINs may require the submission of a HIPAA authorization (as defined in 45 CFR 164.508) or a business associate agreement in order to process an individual access query/pull from an app that has been engaged by, and works on behalf of, an individual.

We would also recommend OCR and ONC clarify in the form of guidance:

- This request process should satisfy the "writing" requirement for sending to third party designees under 45 CFR 164.524.
- Requirement of a HIPAA authorization or other written request in order for individuals to access their health information digitally via a QHIN per the CA is placing a burden on the exercise by an individual of their right under 45 CFR 154.524 and is neither required by, nor permissible under, the HIPAA Privacy Rule (the authorization presented by the app through the API should be a sufficient "writing" to exercise the individual right of access under 45 CFR 154.524).
- The identification and authentication processes required by the TEF are sufficient to meet HIPAA identity proofing requirements under the privacy and security rule provisions for releasing to the individual, absent some indication of a potential flaw or error in those processes.

TEF Language:

Section 6.1.6 – states that "if and to the extent that Applicable Law requires an individual's consent to the Use or Disclosure of his or her EHI," the entity with the direct relationship with the individual must obtain the consent and pass it along to its QHIN, which must maintain it and pass it along to other QHIN's upon request.

CARIN Comments:

ONC should continue to be clear that such consent must be obtained, except in the case of consumer-controlled apps that are responding to a request for information for a Permitted Purpose other than individual access, only in circumstances where it is legally required. (See above for concerns about voluntarily adopted consent policies of covered entities potentially creating obstacles to sharing).

TEF Language:

Section 6.1.7 appears to create a right for individuals to "opt out" of having EHI shared through a QHIN.

CARIN Comments:

ONC should provide more clarity here, for example, if this section creates a new "opt-out" right with respect to exchanges via QHINs versus referring to any legally required consents or authorizations.

TEF Language:

Section 6.2.4 requires QHINs to identity proof individuals and allows QHINs to supplement identity information by allowing Participant staff to act as trusted referees.

CARIN Comments:

While we support the concept of trusted referees, we strongly caution that the industry will naturally gravitate over time to the path of least resistance. As of now, there are not clear guardrails in the TEF or CA as to when an entity should use a trusted referee and when they should not. Without clear guardrails, we are concerned the industry will lose the ability to ID proof individuals across systems in a trusted way which will cause us to revert to where we are today. We presume that QHINs will only be identity-proofing individuals in circumstances where they have direct relationships with individuals (vs. relying on Participants and/or End Users to identity proof individuals). In talking with industry leaders, we have learned there are many organizations (e.g., delivery systems, vendors, EMR companies, etc.) who are currently planning to issue IAL2 certified electronic credentials. Given this identity-proofing event only needs to happen once every nine years per FICAM standards, there is an opportunity to reduce the long-term burden on individuals and providers while still maintaining identify-proofing standards across systems.

TEF Language:

Section 7.1 establishes an obligation on the part of QHINs to respond to query/pulls for individual access, "provided that the requesting Qualified HIN has adhered to the privacy and security requirements outlined in Section 6." This section also makes clear that QHINs are not required to include individuals as Participants or End Users.

CARIN Comments:

As expressed in our comments above, we have concerns about how individuals (and their personal representatives and caregivers) will be able to access their EHI through the TEF ecosystem, particularly if a QHIN is not required to include them or if the definition of Participant or End User (or the requirements that apply to those categories) do not accommodate consumer-controlled models. We request further clarification from ONC on how entities representing the interests of individuals (vs. covered entities or business associates) will be able to help individuals (or their personal representatives or caregivers) exercise their access rights.

TEF Language:

Section 7.2 – allows individuals to opt-out with QHINs of having their EHI exchanged.

CARIN Comments:

As expressed above, CARIN requests that ONC clarify that individuals may opt-out of having their information exchanged via QHINs for the Permitted Purposes but may still leverage a QHIN to exercise their individual right of access (or have that right exercised by a personal representative or caregiver).

TEF Language:

Section 9.3 requires QHINs, Participants and End Users to report failure to abide by the CA to ONC or OIG.

CARIN Comments:

CARIN supports this provision and suggests adding that QHINs, Participants, and End Users should also report failure to honor requests for individual access to OCR.

USCDI Language:

3.2.1 Each Qualified HIN shall exchange all of the EHI in the data classes in the then Current USCDI to the extent such EHI is then available from its Participants and has been requested and to the extent permitted by Applicable Law.

3.2.2 All Participants of a Qualified HIN that collect and maintain EHI in the data classes included in the then Current USCDI, upon request, shall provide all such EHI to fulfill such request to the extent the EHI is available and permitted under Applicable Law

CARIN Comments:

We would recommend including the **FHIR encounter resource on the proposed v1 list** rather than being on the candidate v2 2019 list. The encounter resource is essential to add critical clinical context to all of the other data the patient receives. Individuals want to know which visit the labs, meds, vitals, etc., were related to especially with the addition of clinical notes.

Additionally, while we applaud the ONC's efforts to encourage technical standards to make clinical notes available to individuals, by default the majority of health systems typically expose very few clinical notes to individuals. Thus, we would like to see the ONC consider ways to encourage health systems to expose more clinical notes (e.g., initiatives like OpenNotes) to include full H&Ps, DC summaries, progress notes, visit notes, etc. based on the appropriateness of each use case and what is the minimum necessary based on the HIPAA Privacy rule. We would encourage the ONC and the RCE to provide more clarify on both the depth and breadth of each use case.

USCDI Language: (Page 6, Footnote 3) Is updating data formats and APIs to accommodate new data classes in the exchange of EHI within 12 months of their adoption feasible for plans that are participants of qualified HINs?

CARIN Comments:

Within the CARIN Alliance, many payers believe they may not have the data necessary to fulfill these requests as the data classes unfold, but that doesn't preclude the payer community from supporting this requirement. The payer community believes this may need to be a new cost of doing business otherwise they may not be allowed to participate in a QHIN.