June 17, 2019

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.

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/Promoting Interoperability API 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.

- We believe numerous aspects of the technical infrastructure in the TEF, including the concepts of QHINs and other centralized data entities, are not consistent with a modern internet-based, cloud-enabled economy. We believe building or continuing to rely on large, healthcare specific data silos would be taking a significant step backwards from the numerous positive advancements we are making to rebuild the health IT infrastructure based on modern internet technologies like APIs and open authentication standards. **Therefore, we would strongly recommend the ONC review and reconsider the proposed technical infrastructure and recommendations related to QHINs, etc. and how they are defined in the 2nd version of the TEF with the RCE and 'stakeholder review' board (as defined below) once the RCE has been selected before moving forward.** We believe we can build on the substantial progress already made by established trusted exchange frameworks for document exchange and the work in progress to expand interoperability efforts to API based access and exchange.

- 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 Common Agreement (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.

Ryan Howells
Principal, 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 from the covered entity 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.

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	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
ability or 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. An "On-Ramp" for Data Exchange

The TEF and the Common Agreement seek to scale health information exchange nationwide and ensure that HINs, health care providers, health plans, individuals, and many more stakeholders can access real-time, interoperable health information.

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 or health plan 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 health information 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 agrees with this section of the document assuming QHINs are the recognized preferred technology vehicle for exchanging the data. 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. We also believe the most accurate and effective path for consumers to access their data is directly from the data source rather than through an intermediary.

TEF LANGUAGE: The RCE will establish a process to continuously identify new standards and use cases to add to the Common Agreement and will convene virtual public listening sessions to allow the industry to provide objective and transparent feedback around the development of updates to the Common Agreement. ONC will have final approval of the Common Agreement and all subsequent updates.

CARIN COMMENTS: As discussed in a separate submission, we support the application of The Sequoia Project, Carequality and RTI International to be the Recognized Coordinating Entity for the Trusted Exchange Framework and Common Agreement. We believe that this group, in collaboration with other members of the health care community including CARIN, is well situated to advance consumer access to health care information and interoperability broadly. Consistent with our previous comments, we plan to work collaboratively with the Sequoia group to advance consumer-directed exchange use cases and address unique patient needs.

Rather than the RCE simply "conducting listening sessions", we believe the RCE should include a "stakeholder board" that meets on a regular basis and includes a broader set of stakeholders including the standards community, health plans, pharmaceutical companies, patient and caregiver community, cloud and consumer platforms, and others. The meetings would be led and managed by the RCE and include ONC participation. The stakeholder board's meetings would be open to the public and its recommendations would be included in the public record. We believe the creation of this stakeholder board could be created by identifying and appointing representatives from industry-led consensus making organizations like CARIN, HL7, HIMSS, DaVinci, Argonaut, the Center for Healthcare Interoperability, and others who more broadly represent the entire stakeholder community who would be considered an HIN or who would handle EHI. This is important because the topics and issues the RCE will be addressing in the future require a much more significant representation from broader industry and non-industry stakeholders who could be affected by these policies. We believe this type of an approach can build on what has already been achieved rather than building a separate, new framework that participants would need to migrate to.

Appendix 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 not impede the ability of patients to access and direct their own Electronic Health Information to designated third parties as required by HIPAA.
4. Qualified HINs should provide a method by which individuals can exercise meaningful choice regarding the exchange of EHI about them and ensure that such individual's choice is honored on a prospective basis, consistent with applicable law.

CARIN COMMENTS: As we have previously commented, the CARIN Alliance believes 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. The CARIN Alliance is acutely focused on the ability of consumers to advance their goals through the use and sharing of their health information. Requiring QHINs to provide a method by which consumers can exercise choice and control of their information is critical to this activity as well as ensuring appropriate privacy. We thank the ONC for including this updated requirement and feel it consistent with the recommendations we made to your first draft of the TEF.

As we noted in our last comment, 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. We appreciate your notice that QHINs, Participants, and Participant Members who provide Individual Access Services must publish and make available a written notice describing their privacy practices that mirrors the Model Privacy Notice.

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: "HINs who maintain EHI should (1) enable individuals to easily and conveniently access their EHI; (2) enable individuals to direct their EHI to any desired recipient they designate; 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 at virtually no cost.

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.

TEF LANGUAGE: This principle is consistent with the HIPAA Privacy Rule, which requires covered entities to provide PHI in the form and format in which they request it, if it is readily producible in that form and format.

CARIN COMMENTS: As previously noted in our comments to the first draft of the TEF, 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: As noted in previous 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: Much like the HIPAA law provisions on individuals' access to their health information are important, for purposes of this Principle, HINs should not limit third party applications from accessing individuals' EHI via an API when the application complies with the applicable data sharing agreement requirements and the individual has directed the entity to disclose a copy of ePHI to the application. Likewise, it is also important for individuals to be able to obtain information about how their EHI has been used and disclosed. 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.

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 2019. 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 consumers. As you know, we are working with payers to develop a commercial and MA version of the CMS Blue Button implementation guide which can be found here (https://build.fhir.org/ig/HL7/carin-bb/index.html). 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.

Appendix B – Minimum Required Terms and Conditions for Trusted Exchange

General Comments

The CARIN Alliance agrees with the ONC in 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(s) 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, in conjunction with the "stakeholder board" (as mentioned above), 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 marketplace.

MRTC Language:

2.2.3: Individual Exercise of Meaningful Choice. Each QHIN shall respect the Individual's exercise of Meaningful Choice by requesting that his or her EHI not be Used or Disclosed by a QHIN unless EHI is required by Applicable Law to be Used or Disclosed by the QHIN. However, any Individual's EHI that has been Used or Disclosed prior to the Individual's exercise of Meaningful Choice may continue to be Used or Disclosed for an Exchange Purpose. Each QHIN shall process each exercise of Meaningful Choice from any Individual, or from Participants or Participant Members on behalf of any Individual and communicate the choice to all other QHINs within five (5) business days after receipt in accordance with the requirements of the QHIN Technical Framework. The QHIN shall post instructions on its public website explaining how an Individual can exercise Meaningful Choice. The QHIN shall not charge Individuals any amount for their exercise of Meaningful Choice or for communicating it to the other QHINs.

CARIN Comments:

As we comment above, we strongly support the ability of each individual to exercise meaningful choice over how their health information is used and disclosed. As we commented during the first round of TEF activity, in the ONC Information Blocking rule, and the CMS Patient Access rule, consumers must have control over how their information is used and disclosed, subject to applicable state and federal law. We strongly support this requirement for QHINs.

We also strongly support the ability of a consumer to access their entire longitudinal health information from any provider or health plan in the country at no cost to the consumer or the consumer's third party application which is the main vehicle by which a consumer will access their digital health information. We also strongly support the ability to use their third-party application to redirect their information to any third-party of their choice, including other QHINs, at no charge to the consumer. As consumers navigate through the health system, they should always know where their data is being directed and how their data is being used based on their own personal preferences. We also believe this language should be required across all health care data use agreements.

MRTC Language:

2.2.4: Processing of Individual Access Services Request.

(i) An Individual User may assert his or her right of Individual Access Services with respect to a QHIN if it has a Direct Relationship with the QHIN. The QHIN may require such Individual User to assert his or her right to Individual Access Services to EHI in writing and may require such Individual User to use the QHIN's own supplied form, provided that the use of such a form does not create a barrier to or unreasonably delay the Individual User from obtaining access to the EHI. Each QHIN shall provide Individual Users with the option of using electronic means (e.g., e-mail or secure web portal) to assert their rights for Individual Access Services to EHI.

(ii) Each QHIN that receives a request for Individual Access Services from an Individual with whom it has a Direct Relationship shall provide such Individual with Individual Access Services with respect to his or her EHI regardless of whether the QHIN is a Covered Entity or Business Associate; provided, however, that if the Individual wants the EHI to go to a third party, the Individual has satisfied the conditions at 45 CFR § 164.524(c)(3)(ii) as if it applies to EHI.

(iii) When the QHIN is acting as a Business Associate and the request for Individual Access Services is received by a Covered Entity that directs the QHIN to satisfy the Minimum Required Terms & Conditions (MRTCs) Draft 2 44 request, then the QHIN may respond to a request for Individual Access Services if permitted or required by the terms of the applicable Business Associate Agreement.

(iv) A QHIN is prohibited from requiring the submission of a HIPAA authorization (see 45 CFR 164.508), or a Business Associate Agreement (see 45 CFR 164.504(e)), in order to process a request for Individual Access Services from a Participant who provides Individual Access Services that has been selected by the Individual User who is requesting EHI for Individual Access Services.

(v) With respect to a QHIN Query for Individual Access Services, the response shall be provided as required by these terms and conditions regardless of whether it was prompted by (a) the Individual User; or (b) a QHIN, Participant, or Participant Member who provides Individual Access Services and has been selected by the Individual User who is requesting EHI for Individual Access Services.

CARIN Comments:

We appreciate the significant work that ONC has done to clarify and advance an individual's rights to pull data from QHINs and support this section as is currently written. We especially appreciate the clarity that you have provided in this section on:

1. Requirements on HIPAA authorization forms and BAAs;
2. Forms and formats that may be required to assert the individual access request;
3. Clarity on how and individual may direct their information to a third-party; and
4. How a QHIN interacts with a CE with whom it has a BAA.

As previously noted, we believe that individual consumer access can be facilitated by the RCE and QHINs but note the need for clear rules and expectations for how individuals will interact with the QHIN. We also believe the ONC should expand the definition of 'in writing' to include additional electronic means supported in the ONC's proposed information blocking rule. These include the use of digital authentication and authorization tools and technologies such as OAuth 2.0, Open ID Connect, etc. The CARIN Alliance believes if a user is securely authenticated using SMART on FHIR or presents an identity authentication level 2 (IAL2) credential to a QHIN or other appropriate entity that should be sufficient to assert and record his or her right of Individual Access Services. There should not be a

requirement or separate process for capturing 'in writing' an individual user's request for their own health information.

In Part B of the TEF, the Minimum Required Terms and Conditions, 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.

MRTC Language:

2.2.10 Notice to individuals.
When a QHIN has a Direct Relationship with an Individual, then the QHIN shall be responsible for notifying the Individual of the mandatory provisions stated in Section 9 by posting such mandatory provisions on its public website.

CARIN Comments: We support this requirement for QHINs to provide privacy and security information on its public website.

MRTC Language:

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 as proposed 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. Otherwise, we support this section.

We also support the phrase 'or any then applicable standards adopted in the future by HHS'.[1] The CARIN Alliance is working with industry stakeholders on an approach to improve and hopefully eliminate the 'patient matching' problem in health care through our digital identity workgroup which seeks to federate IAL2 token credentials across the health care ecosystem. We believe taking a person-centric, mobile-first approach to digital identity will help to

[1] We recommend this be done through an updated QTF

solve the institution-centric, demographics-first approach currently used in health care which is replete with data entry errors. We look forward to working more directly with HHS and the ONC on advancing these open standards.

MRTC Language:

3.1 Patient Demographic Data for Matching. Each QHIN shall send and receive all of the "patient matching data" so labelled and specified in the QHIN Technical Framework when and to the extent that all of the requirements of Section 3.3 are satisfied.
3.2 Data Quality Characteristics. To help confirm that QHINs exchange accurate patient demographic data that is used for matching, QHINs shall annually evaluate their patient demographic data management practices using the then applicable PDDQ Framework. The first such evaluation shall be conducted within eighteen (18) months after the QHIN has executed the Common Agreement.
3.3 Minimum Necessary Requirements. A QHIN shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI and when the QHIN requests EHI in the context of the Common Agreement. The Minimum Necessary Requirements shall apply to a QHIN when it requests, Uses, or Discloses EHI. Any provisions in the HIPAA Rules (e.g., 45 CFR § 164.514(d)) that include conditions shall also apply to the QHIN when Using, Disclosing or requesting EHI if such provisions are applicable. In addition, the Minimum Necessary Requirements do not apply under certain circumstances set forth in the HIPAA Rules including the following: (i) a Disclosure of PHI to or request by a health care provider for Treatment; (ii) a Disclosure to an Individual who is the subject of the information; (iii) a Disclosure pursuant to an Individual's authorization under 45 CFR § 164.508; or (iv) Disclosures that are required by law as described in 45 CFR § 164.512(a). These exclusions apply to a QHIN with regard to EHI.

CARIN Comments:
As we have previously commented, 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. This includes all the information needed to ensure compliance with an identity assurance level 2 (IAL2) trusted credential. Without this information, it will be extremely difficult to identify individuals across systems. We would also echo our comments mentioned in our last comment.

MRTC Language:

5.1.2 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.

MRTC Language:

5.2.2 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.

MRTC 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 the MTRC, 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.

MRTC Language:

Section 6.1.4 – 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:

As we have previously commented, ONC should continue to be clear that such consent must be available, 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).

MRTC Language:

Section 6.2.4 Identity Proofing: Each QHIN's Security Policy shall include the following identity proofing requirements:

I. QHINs. Prior to the issuance of access credentials, each QHIN shall identity proof any staff or users at the QHIN who may initiate a QHIN Query or QHIN Message Delivery at a minimum of IAL2.

II. Participants/Participant Members. Prior to the issuance of access credentials, each QHIN shall require that Participants be identity proofed at a minimum of IAL2. Each QHIN also shall require each of its

Participants to identity proof its Participant Members at a minimum of IAL2 prior to the issuance of access credentials.

III. Individual Users. Each QHIN shall require that Individual Users with whom it has a Direct Relationship be identity proofed at a minimum of IAL2 prior to issuance of access credentials by the QHIN. The identity information may be supplemented by the Participant or Participant Member acting as authoritative sources by using knowledge of the identity of the Individuals in accordance with written policies and procedures. Such policies and procedures must be commensurate with the risk of incorrect identity proofing (e.g., procedures for applicants receiving credentials to access their medical information may be less rigorous than procedures used for applicants receiving credentials that can be used to access medical information on multiple patients). For example, IAL2 identity proofing for an applicant receiving credentials to access to his or her own medical information can be accomplished by any two of the following:

a. physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges;
b. comparison to information from an insurance card that has been validated with the issuer (e.g., in an eligibility check within two days of the proofing event); and
c. comparison to information from an electronic health record (EHR) containing information entered from prior encounters.

All personally identifiable information collected shall be limited to the minimum necessary to resolve a unique identity and the QHIN shall not copy or retain such personally identifiable information.

CARIN COMMENTS: We appreciate the significant work the ONC has done to address the topic of identity and for including the CARIN Alliance's identity and authentication recommendations again in this version of the TEF. We are very supportive of this language with one exception. We believe the language isn't totally clear after the first sentence. Therefore, **the CARIN Alliance recommends everything after the first sentence in Section III – Individual Users should be removed** to allow for a mix of both federated and centralized approaches.

The first sentence makes a declarative statement that each QHIN shall require individual users to be identity proofed at a minimum of an IAL2. That language is clear, accurate, and we're very supportive of it. We believe no other additional information is required because unfortunately, the language then becomes a bit murky.

The paragraph continues by saying 'the identity information *may be supplemented* by the participant or participant member acting as authoritative sources by using knowledge of the identity of the individuals in accordance with written policies and procedures.'. The word *supplemented* implies there *may* be additional information provided *in addition to* the IAL2 digital credential. But then the language says, 'IAL2 identity proofing for an applicant receiving credentials to access his or her own medical information can be accomplished by any two of the following. . . "

This additional language, which seems to indicate *either* a trusted referee (which we assume is what the ONC meant with the language) *or* an IAL2 credential is acceptable. Once an individual is identity proofed at an IAL2 level and receives a digital credential, there isn't a need for a 'trusted referee'. The CARIN Alliance believes the concept of a trusted referee is not needed and in fact may be detrimental to the intent of this provision. If both options are provided to a health care entity, most health care entities will take the path of least resistance which in this case is the 'trusted referee' path. We believe in today's health care environment one of the major reasons we have 'patient matching' issues is because we have a manual 'trusted referee' process today.

As we will indicate below, IAL2 certified digital credentials are *already being used in production* by multiple public and private sector entities. As such, the CARIN Alliance believes everything after the first sentence in Section III – Individual Users should be removed.

As we noted in our previous 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 username 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 and health plan 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. Other public and private sector digital identity providers include: Healthcare.gov, Login.gov, Apple, Google, ID.me, AARP, and numerous others.

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. The CARIN Alliance and its members are actively developing technologies to support these capabilities. 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.

We also strongly recommend that 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.

MRTC Section 9:

9.1 Individual User Access to EHI. An Individual User who has a Direct Relationship with a QHIN, Participant, or Participant Member, may exercise his or her right to Individual Access Services by sending a written notice to said QHIN, Participant, or Participant Member. If required by said QHIN, Participant, or Participant Member, the Individual User shall be responsible for completing the QHIN's, Participant's or Participant Member's own supplied access form provided that the use of such a form does not create a barrier to or unreasonably delay the Individual User from obtaining access to the EHI. Such Individual Users shall have the option of using electronic means (e.g., e-mail, secure web portal) to assert their rights for Individual Access Services to EHI.

9.2 Individual Use or Disclosure of EHI. Individuals shall have the right to Use or Disclose their own EHI without any limitations.

9.3 Identity Proofing. Prior to the issuance of access credentials, an Individual User shall be required to verify his or her identity at a minimum of IAL2 with the QHIN, Participant, or Participant Member to whom the Individual has a Direct Relationship.

9.4 Authentication. Prior to initiating Individual Access Services, an Individual User shall be required to authenticate at AAL2 with the QHIN, Participant, or Participant Member with whom the Individual has a Direct Relationship.

9.5 Right to Receive Summary of Disclosures of EHI.

9.5.1 Right to Request Summary and Applicable Period. As described below, Individuals shall have the right to receive a summary of Disclosures of EHI for applicable Exchange Purposes in the context of the Framework Agreements for up to a period of six (6) years immediately prior to the date on which the summary of Disclosures is requested. Individuals may submit requests for a summary of Disclosures to any QHIN, Participant, or Participant Member with which the Individual has a Direct Relationship. QHINs, Participants, and Participant Members shall provide the summary within sixty (60) days after receiving the request and shall provide an electronic means for an Individual to submit such requests. For Covered Entities, this obligation may be met by complying with the requirements of 45 CFR § 164.528.

9.5.2 Content of Summary. The content of the summary of Disclosure(s) shall contain the following information: (i) date of the Disclosure(s); (ii) name of the entity or person who received the EHI and, if known, the address of such entity or person; (iii) brief description of the EHI disclosed; and (iv) brief statement of the purpose of the Disclosure(s) that reasonably informs the Individual of the basis for the Disclosure(s) or, in lieu of such statement, a copy of the written request for the Disclosure(s).

9.5.3 Exceptions. A summary of Disclosures shall not be required for the following Disclosures: (i) for treatment, payment and health care operations (each as defined in the HIPAA Rules); (ii) to an Individual of his or her own EHI; (iii) pursuant to an Authorization under 45 CFR 164.508 executed by the Individual; (iv) to correctional institutions or law enforcement officials; (v) for national security or intelligence purposes; and (vi) if providing the summary of Disclosures of EHI would be in violation of Applicable Law.

CARIN Comment:

The CARIN Alliance appreciates the comprehensive discussion of the individual rights and obligations that consumer have under the TEFCA. We believe that this section, in addition with your discussion in 2.2.4 will go far in providing QHINs and Participants with clarity in interacting with Individual Users.

USCDI Language:

2.2.1 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.

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.