We are supportive of the goals outlined in the 21st Century Cures Act to establish a Trusted Exchange Framework and Common Agreement for a national health information exchange. Interoperability remains a priority and we appreciate the ability to comment and help shape the future advances of a national health information exchange.

We are supportive of the notion of a Qualified Health Information Network to be able to facilitate a network to network exchange so that an organization can on-board once, to gain access to many. We hope that the complexity of the certification process does not limit the competition which will ultimately drive associated exchange costs down allowing for data to become more liquid.

In order to accomplish this goal and to have a greater impact, we believe that the focus should be on leveraging and promoting existing capabilities that are working well and advancing health information exchanges happening today. There have been advances in nation-wide Interoperability within the industry as seen with organizations such as CommonWell. In order to propel these advances further, we must ensure that the requirements outlined are clear and concise. We are supportive of the principles outlined in the MRTC and the requirements of the QTF but we believe more clarity is needed for TEFCA to be successfully adopted.

Again, ensuring that existing capabilities are leveraged wherever possible will allow a QHIN to be able to implement within the 18-month timeline. We are concerned that some of the requirements outlined in this draft could cause significant development work for the QHIN and possibly its participants, thus causing delays. In lieu of requiring a very narrow set of requirements, we should rather be taking a look at some of the frameworks that already exist today that, in the end, can achieve the overall goal.

Although we believe in a defined set of requirements to facilitate national health information exchange, the fewer unnecessary barriers for a QHIN and its participants to adopt will help facilitate a broader adoption.

We appreciate the approach to be able to switch organizations to fulfill the RCE responsibilities. For continuity and stability, we offer consideration of an approach that does not use a four-year renewable term, but rather an undefined period with termination clauses for non-performance. We believe this offers more assurances to participants on the consistency and longevity of the processes, staffing, and approach.

Thank you for this opportunity to share our input. We look forward to continuing to support efforts toward enhanced exchange of health data.

## Appendix 1:
## The Trusted Exchange Framework
## (TEF Draft 2)
*Page 24*

**Principle 1- Standardization: Adhere to industry and federally recognized technical standards, policies, best practices, and procedures**

We are supportive of adhering to recognized standards, as it is essential to enabling health exchange among many disparate organizations and vendor systems, as long as the standards are mature in the industry. These standards should align with 2015 certification. This is the baseline that currently exists and large investments have already been made to ensure that all certified systems have these capabilities inherent in their systems. We should be leveraging and promoting standard interoperability that works well now. We appreciate the mention of USCDI and the alignment with the 21st Century Cures Information Blocking rule. Any immediate change in standards that go beyond current deployment could cause barriers for participants.

We again support leveraging existing capabilities wherever possible. Not every participant will use the technology at the same level so we encourage ONC to not impose requirements beyond their specific use cases.

---

**Principle 2 - Transparency: Conduct all exchange and operations openly and transparently**

We support the proposal to make terms, conditions, and contractual agreements that govern the exchange of EHI easily and publicly available.

We support the proposal to specify and have all HINs agree to the uses and disclosures for exchanging EHI.

We agree with the proposal to publish, keep current, and make publicly available the HIN's privacy practices. However, more defined standards are needed in order for patients to document their "meaningful choice" and have that adhered to. Standards should be identified and clearly defined.

We agree that when necessary, conduct of any arbitration processes with other HINs in an equitable, transparent manner.

---

**Principle 3 - Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange EHI, even when a stakeholder may be a business competitor**

We are supportive of the principle to not seek to gain competitive advantage by limiting access to individuals' EHI which aligns with the information blocking rule.

---

**Principle 4 - Privacy, Security, and Safety: Exchange EHI securely and in a manner that promotes patient safety, ensures data integrity, and adheres to privacy policies**

We are supportive of requiring a more standardized approach to patient matching by itemizing demographic and other information that can be used to match patients with more certainty and have evidence of working in current models.

We recognize the need to use certain demographic data to enhance record matching in the absence of using stronger identifiers. This will improved registration processes and the tools that enhance data quality of the data involved (e.g., standardized data field formats, collection of additional data that has improved matching potential such as phone numbers or other identifiers). However, we suggest that the RCE works closely with the industry to establish minimum data set and standards to avoid sending too much PHI for purposes of identification, which is a security risk in itself.

---

**Principle 5 - Access: Ensure that Individuals and their authorized caregivers have easy access to their EHI**

We are supportive of the general intent of this principle. We do request clarity on the meaning of "unnecessary barriers." We note that as technology evolves and matures, these definitions may change. We suggest that in this context, use of USCDI as a scoping tool and maintaining consistency with information blocking exceptions is appropriate. Data not yet a part of USCDI may not be accessible and should not be considered having "unnecessary barriers" to obtain, even though it falls within EHI. We recommend that ONC and the RCE work closely with the industry to establish reasonable expectations and clarify what would be "unnecessary" in the context of relevant infrastructure and standards.

---

**Principle 6 - Population-Level Data: Exchange multiple records for a cohort of individuals 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**

We recommend that population-level data not be part of phase I, due to the lack of mature standards. We also recommend promoting efforts to begin creating and/or selecting standards in order to reach this population health data goal.

## Appendix 2: Minimum Required Terms and Conditions (MRTCs Draft 2)

***Page 32***

We agree with the overall minimum required terms and conditions, however, we are concerned with the amount of technical work needed for MRTC. The industry will need time to complete the requirements correctly and thus we are concerned about the 18 month implementation period.

**6. Privacy, Security, and Patient Safety**

We are generally supportive of the proposal to address the privacy and security of an individual and how to handle consent. We request clear guidance on how to handle privacy concerns and how to adequately segment information based on meaningful choice. We have concerns that the standards mentioned in ONC Information blocking rule have not reached an appropriate level of maturity.

## Appendix 3:
## Qualified Health Information Network (QHIN) Technical Framework (QTF Draft 1)
*Page 70*

We want to stress that the new framework should be based on existing capabilities. Currently the structure available through the CommonWell framework, which is LIVE and exchanging at the national level, utilizing a Record Locator Service. Changing this framework, that has been very successful, may impact the industry negatively and set us back instead of advancing the technology. We are also concerned about the impact on existing local HIE's and their ability to continue serving their community exchanges and costs associated with plugging in into qualified network.

---

**2. Example QHIN Exchange Scenarios**

We recommend that the QHIN exchange should not just rely on IHE profiles but should accept more modern standards such as FHIR. Essentially, we advise that the QHIN should be able to use multiple approaches and protocols. As long as the same end goal is met, the QHIN should be able to broker, accept and do the necessary negotiations to facilitate the exchange.

---

**3. Functions and Technology to Support Exchange**

We support the Certificate Policy approach in general, in the context of document exchange. As we move into other access and exchange, such as data element or data set level exchange, applicable standards and approaches may change.

Regarding ***RfC #1*** we generally support the standards and approach suggested for Secure Channel document exchange, but variations may be required based on the exchange (e.g., document vs. data element/set) while one should not assume a centralized QHIN server to be in place for all use cases or parts of use cases. We strongly support Mutual Authentication between QHINs.

The currently accepted industry standards for encryption of data are always changing. As time progresses, older cipher suites depreciate, and at times a serious vulnerability is found which necessitates dropping an acceptable protocol or cipher suite rather quickly. We are happy to see that Draft 2 recommends TLS1.2 or better, but we think it should also state that there must be a commitment to maintaining systems to the currently acceptable TLS standards without unreasonable delay. Currently, acceptable TLS standards should be those defined as acceptable by the Internet Engineering Task Force (IETF).

---

**Requests for Comment**

As an EHR vendor, we are focused on how we will communicate with our QHIN. With many networks currently document based, we encourage ONC to progress towards a RESTful exchange. We also urge ONC to build upon existing (aspiring) QHIN capabilities, and not to impose barriers on QHIN to QHIN communication.

Regarding ***RfC #2*** we agree that more specific guidance regarding User Authentication is required than provided in the current draft.

Regarding ***RfC #3*** we suggest considering all QHIN approaches. However, we note that not all consent related assertions have been widely implemented yet. Further work is required to establish a roadmap for adoption, while remaining sensitive to the general complexities that still need to be addressed to make data segmentation and consent management a practical, manageable process across stakeholders.

Regarding ***RfC #4*** we suggest not assuming a central configuration for Query. Therefore a QHIN would not "fail" to resolve, but it is the QHIN environment that fails. We should allow the QHINs to determine where in its configuration this is identified, as long as it is consistently and appropriately communicated to the other QHIN using "QHIN level" standards.

Regarding ***RfC #5*** we agree there should be a minimum, but we suggest not finalizing queries/parameters before the RCE, in collaboration with (aspiring) QHINs, Participants and Participant Members, have the opportunity to work through this.

Regarding ***RfC #6*** we agree that, while the IHE profiles do allow for more granular metadata to support further queries, the logical place to explore this capability is using FHIR based API access queries. We recognize there may be further need to query for documents that contain "xyz," but that would require substantial implementation guidance and deployment. We suggest that pursuit of these capabilities, beyond what current metadata practices support and what FHIR based APIs can support, be left to the market to drive and then prioritize in the RCE. This approach can then also consider the privacy concerns associated with expanding the document metadata content, with certain data that now will be further exposed.

Regarding ***RfC #7*** we support a minimum data set using standardized formats where available, adding strong identifiers, while also recognizing the need for improved registration processes to improve the quality and completeness of that data set.

Regarding ***RfC #8*** considering the variety of use cases, the QHIN should not be required to have a centralized patient index. Rather it should have the ability in its network "collectively" to resolve identities based on an agreed-to data set that is used across QHINs. As indicated at the recent CARIN/ONC/CMS Patient Identity Summit, there are opportunities to improve on both identity proofing and patient matching. These two are closely related. The RCE should work closely with (aspiring) QHINs, Participants, and Participant Members to address identity proofing processes that enable participants to improve trust in others' identity proofing performed, thus improving opportunities to reduce duplication and missed matches from the

start.

Regarding ***RfC #9*** we suggest consideration of reporting on key measures that can highlight opportunities for improvement, sharing of best practices, and perhaps sharing of algorithms, but we do not suggest establishing a common, singular algorithm or process.

Regarding ***RfC #10*** we suggest the use of common query standards for Record Location, but not necessarily a singular architecture/configuration for a singular record locator service per QHIN. We do note that with the advent of patient event notifications, that all record locator services can be informed of those events (subject to applicable privacy law, meaningful choice, and consent directives) to improve on the ability to locate a patient's record.

We suggest that use of record locator services should be encouraged as it has the opportunity to reduce unnecessary requests for data from locations that do not have awareness of that patient. It's important to recognize that certain use cases may still require such queries where the record locator service is not yet expected to be up-to-date, particularly as long as patient event notifications are not widely shared.

Regarding ***RfC #11*** we support the need for directory service, but it should reflect the minimum necessary to fulfill the functions and may only be used for the QHIN participants for purposes of managing/maintaining the network and interoperability. These services should not be used for commercial, marketing, or other competitive purposes.

Regarding ***RfC #12*** we suggest that Individual Privacy Preferences generally, particularly for TPO and covered entities, the opt-out -- in other words, opt-in as the default -- should be preferred where allowed by law. Current experiences with adoption rates and realization of the value of sharing patient health data across stakeholders indicate faster uptake and more benefits.

Regarding a standard for meaningful choice, we suggest consideration must be given to both the format of, the choice and the format/means/need to communicate this choice. Regarding the former, the RCE and ONC may work with OCR to address the appropriate documentation format, while for the latter the RCE may work with (aspiring) QHINs, Participants and Participant Members to determine whether and what data needs to be shared beyond the data source to respect the choice, or whether no data is to flow, to begin with. We recommend clearly delineating the scope of meaningful choice vs. consent directives, as these two are easily conflated.

We recognize that to operationalize privacy preferences, identity proofing, and patient matching are keys to enable the correct data to be disclosed, or not. We note that in the context of maintaining privacy to the level desired, sharing of demographic data for purposes of matching and record location must also be kept to a minimum. Thus, exploration of strong identifiers validated through trusted identity proofers may well provide an opportunity to further protect the privacy of patient data by sharing less demographic and metadata for purposes other than those actually at hand.

TEFCA needs to properly and thoroughly address patient matching and identify what demographic information will be required in order to match patients. Any data that is part of the patient matching requirements should also be included as part of the information included in a Meaningful Choice notice. Without both resolution on patient matching and the required matching information in the notice, a QHIN will not be able to prospectively administer Meaningful Choice reliably.

Regarding ***RfC #13*** we acknowledge challenges with interstate QHIN communications (whether within a QHIN spanning states or across QHIN spanning states). However, also in this context, we note the suggestion to share the minimum necessary from the data source to fulfill the requirements of state law or the patient.

As data needs to be shared, common vocabulary for labeling data at various levels has been reasonably established, but challenges remain with having established, agreed-to mappings between privacy policies and appropriate labeling to enable patients to provide consistent consent directives and for systems to honor those directives as data is communicated when permitted. We also note that, in any case, the burden of maintenance falls with the provider and patient in the Participant Member setting, as the QHIN at large may not even be allowed to be aware of the presence of certain/any data.

We recommend the latest version of the FHIR standard for resource consent.

Regarding ***RfC #14*** we suggest that EHRs have robust audit capabilities. Their audit lists would serve as a solid starting point considering §170.210(h): Audit log content (https://www.healthit.gov/sites/default/files/170%20315%28d%29%282%29%20Auditable%20Events%20and%20Tamper-resistance.pdf). These logs can be used, and should be accessible, to identify bad actors when there is suspicion of abuse. Where deemed valuable to improve auditing, these audit events can be augmented or enriched with further metadata that can be used at the QHIN level. When traffic goes through a centralized QHIN server, similar audit events should be tracked, but not supplant those in place. We do note that, in this environment where we must support cross-state and cross-border data access/exchange, great care must be given to the definition and use of audit events, as they may contain information that cannot be shared across borders.

Regarding ***RfC #15*** we suggest that error messages should be specified by RCE in collaboration with the (aspiring) QHIN, Participant, and Participant Members as appropriate. Acknowledgment and error messaging are as critical as the underlying message/service call/document itself to enable reliable delivery of the data request/response and react correctly to any interruptions. Therefore, establishing a standard set of error messages is appropriate to be within scope.