33 W Monroe, Suite 1700
Chicago, IL 60603
swillis@ehra.org
Phone: 312-915-9518
Twitter: @EHRAssociation



June 17, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker,

On behalf of the more than 30 member companies of the Electronic Health Record (EHR) Association, we are pleased to offer our comments to the Office of the National Coordinator for Health Information Technology (ONC) on Draft 2 of the Trusted Exchange Framework and Common Agreement (TEFCA). We appreciate this opportunity to provide input on this effort to enable exchange of patient health data across networks.

EHR Association members serve the vast majority of hospitals and ambulatory care organizations that use electronic health records (EHRs) and other health information technology to deliver high quality, efficient care to their patients. Our core objectives focus on collaborative efforts to accelerate health IT adoption, advance interoperability, and improve the quality and efficiency of care through the use of these important technologies.

We continue to strongly support the intent and goals of the 21st Century Cures Act to enable nationwide data access and exchange in order to more effectively coordinate patient care. EHR developer support is evident from EHR Association members' participation in a wide range of initiatives that have substantially progressed since the Cures Act was enacted in 2016, enabling our healthcare customers to connect:

- To Health Information Networks (HIN), including regional HIEs and national networks such as eHealthExchange and CommonWell
- Across HINs that are part of the Carequality framework
- Directly with other providers in or outside any of these networks using the Direct Protocol

Millions of documents are queried using various query types (broadcast or targeted, brokered or directed), and are also sent to specific providers. Initiatives now in progress go beyond document exchange and will enable scaling of HL7® FHIR®-based API access to national network levels.

We appreciate the support and drive that ONC has demonstrated in its efforts to enhance interoperability at a national level, and we look forward to ongoing collaboration to continue this progress. We find that this second draft of TEFCA increases the clarity of the proposed approach in many areas in comparison to the first draft, yet it still leaves challenging questions and need for clarification.

In particular, the EHR Association is unclear how this proposal enables continued growth and support of current initiatives. We see this proposal as an independent effort, rather than complementary to existing initiatives, thus resulting in duplicative efforts that distract from current initiatives, slow progress, and creates uncertainty for all stakeholders on where to focus.

Existing private-sector exchange efforts such as Carequality, CommonWell, eHealth Exchange and networks established in different regions have come a long way, moving from how to exchange data to which types of data to exchange. We believe that building on established networks and processes like these is preferable to developing what would be essentially a duplicate framework, as is proposed in Draft 2 of TEFCA. The introduction of a new framework could prove disruptive to current levels of interoperability and/or cause a hesitancy to connect to existing initiatives until TEFCA is well established.

EHR Association members remind ONC that Congress intended for TEFCA to be a voluntary, non-prescriptive approach to addressing governance and trust. However, the proposed approach is more prescriptive; through both the proposed Minimum Required Terms and Conditions (MRTC) and the QHIN Technical Framework (QTF), it creates a framework parallel to existing trusted exchange frameworks/networks. Because other programs and initiatives, such as potential information blocking exceptions, might *require* participation in the TEFCA defined framework, this approach introduces effectively a mandatory transition to the TEFCA defined framework, contrary to Congressional intent.

Our feedback is based on the experience that our members have gained from their active participation in existing interoperability initiatives. While we have provided detailed comments, our key points may be summarized as follows:

- EHR Association members support the six principles outlined and the adjustments made between TEFCA Draft 1 and Draft 2 to address certain aspects in either the MRTC or the QTF. These principles are generally recognized in the existing major national networks.
- The EHR Association appreciates the separation of the technology-related sections in the initial Common Agreement, which will enable separate development and evolution without the need to revisit legal agreement language when changes are limited to technology only.
- The EHR Association understands and appreciates that the QTF is representative of an early draft and is expected to be further defined and developed by the RCE in strong collaboration with (aspiring) QHINs, Participants, and Participant Members in an open, public format. Such collaboration is essential to achieve the level of consistency, buy-in, and value to progress to a viable, practical QTF.

However, the principles, MRTC, and accompanying Users Guide diagrams still imply a certain architectural approach—reflected in the exchange modalities and further re-enforced by the QTF—that envision a centralized, brokered exchange model. Currently, we see effective exchange across HINs where some are strongly brokered, others more federated, yet all capable of interacting. Also, we note that with the advent of HL7 FHIR-based API access to data elements/sets, the approaches may vary from the document exchange approach.

We suggest clarity that, within and across QHINs, there is not a requirement that all data queries, responses and message deliveries must physically flow through a central QHIN server. For certain steps in the exchange, data may be brokered through a central QHIN server, while for subsequent steps, it may not. Such variations should be addressed through the QTF; i.e., when centralized brokering *is* required to support the use case, and when it does not matter. We make various suggestions in our detailed comments.

- EHR Association members appreciate the widening of HINs that are eligible to become a QHIN. However, the HIN definition used in TEFCA mirrors the overly broad definition that ONC proposed in its recent Cures Act NPRM, and includes a number of organizations that do not seem to fit the intent of a health information network (e.g., organizations such as HL7 or CARIN who are valuable contributors, but not health information networks), or are outside the intended scope of stakeholders, e.g., credit card companies.

  If ONC does not finalize a narrower definition, it will need to further clarify the eligibility requirements for a HIN to pursue QHIN designation.

- EHR Association members are concerned with the proposed approach that MRTC language and, once approved, Additional Required Terms and Conditions (ARTC) are intended to be adopted as-is, all together. This raises substantial questions around a number of topics:
  - Proposed terms are marginally different from existing language, thus raising the question why existing language would have to be replaced.
  - As ONC and the RCE work to implement TEFCA, they should clarify the relationship between the Common Agreement and existing exchange agreements. We appreciate ONC's removal of the disruptive provisions from Draft 1 that required entities to exclusively engage in exchange via the TEF but remain concerned with how the proposed TEF would work in parallel/complementary to existing exchange agreements.
  - For example, consider the hypothetical scenario where a HIN elected to pursue QHIN designation. It would be appropriate for entities engaging in exchange according to that HIN's existing terms to continue doing so during the onboarding process. Then, the HIN's "Participants" could elect to complete the TEFCA Participant onboarding process and exchange according to the terms of the Common Agreement. But, if not all participants within that HIN or other HINs were prepared to onboard on the same timelines, exchange should not be disrupted.

  Therefore, we strongly suggest that ONC and the RCE work in tight collaboration with (aspiring) QHINs, Participants, and Participant Members to develop a clear roadmap on how a transition is to occur without interruption of information exchange already underway. That should include consideration of staging the introduction of new terms with transitional/grace periods, as well

as being able to consider existing agreement language to be sufficiently consistent with the intent of the MRTC and ARTC to not require replacement. We do not believe that comment periods and listening sessions are adequate tools to develop such roadmaps. A workgroup approach, where key stakeholders can be directly at the table through interactive discussions, is more effective.

We recognize that having a consistent, common set of agreement language is ideal; if we were to start from ground zero that could be used as a starting point. However, considering what is in place and works, a carefully crafted roadmap to introduce new MRTCs and ARTCs is essential to avoid unnecessary disruptions. Until and unless there is clarity on this approach, including the benefits to the stakeholders as to why a replacement strategy is chosen, we are concerned that current progress will slow or too few will voluntarily adopt TEFCA lest they are required to adopt it in order to "check the box" to participate in a particular program or contract.

- The current proposed QTF technology stack is not sufficiently specific enough to be introduced as-is. While the QTF is clearly identified as a draft and subject to further definition by the RCE in collaboration with (aspiring) QHINs, Participants, and Participant Members, EHR Association members are concerned that the approach has a risk of re-creating/establishing guidance that already has traction. We suggest clarifying that the RCE can choose an existing, commonly used technology stack as the starting point, rather than having to restart from zero. This would minimize HINs having to support yet another flavor of technology to enable connectivity with those on TEF vs. those not yet on TEF.
- The EHR Association is concerned with the proposed timeline of 18 months for a QHIN to have implemented the proposed requirements. If the scope is intended to mean that within 18 months of a HIN becoming a QHIN that all technical capabilities are to be in place and all agreements with its participants and their members at the time the HIN became a QHIN are to be converted to Participants and Participant Members—with all having therefore signed the applicable ARTCs and MRTCs -- then this seems unrealistic. For clarity and manageability of the rollout, we recommend that timelines be established by the RCE based on specific topics considering the then-current state of the effort needed to implement that topic. Depending on the choice of replacement strategy (with varying degrees of transition steps) or progression of current initiatives, the timelines may vary.
- EHR Association members 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.
- Overall, the EHR Association suggests that wherever possible an outcomes-focused approach be applied that considers the available connections, successful queries and deliveries, privacy/security adherence, and conformance to standards as key drivers rather than a prescriptive approach without the benefit of iterative learning.

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

Sincerely,

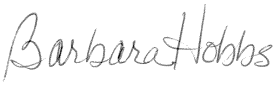
Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Sasha TerMaat
Vice Chair, EHR Association
Epic

**HIMSS EHR Association Executive Committee**

David J. Bucciferro
Foothold Technology

Hans J. Buitendijk
Cerner Corporation



Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
Evident

Emily Richmond, MPH
Allscripts/Practice Fusion

Courtney E. Tesvich, RN
Nextech

**About the EHR Association**

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

# Detailed Comments of the HIMSS Electronic Health Record Association on the Trusted Exchange Framework Draft 2

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

EHR Association members appreciate and support the basic principles outlined and described. These principles are largely already in place in existing national frameworks/networks, and reinforcing those through TEF is very helpful.

We suggest that ONC and the proposed RCE work with stakeholders to identify key metrics that measure success toward the goals of a trusted exchange framework (e.g., number of connected endpoints per use case, number of transactions by type, time to connect to "all") and adherence to its principles.

---

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

EHR Association members support the principle to use standards-based approaches, which reflect industry consensus in key areas. This is particularly important for interoperability standards, as standards enable access and exchange of data with high fidelity.

We agree with the inclusion of USCDI as the basis for the minimum data set, with associated vocabulary that can be accessed and exchanged. This would promote consistency with ONC's certification approach, while creating a predictable glide path for nationally scalable data access and exchange. It would further enable consistency in expectations across data held by covered entities and non-covered entities alike that participate in the trusted exchange framework.

In the long term, USCDI will expand targeting the Designated Record Set/Protected Health Information set of data classes rather than the substantially larger definition of Electronic Health Information (EHI), as defined in the ONC's Information Blocking and Certification proposed rule.

In general, we agree that the certification program, SVAP-designated standards/ implementation guides within the ISA, as well as the full ISA, are good sources to consult before selecting a specific standard or implementation guide for the use cases the trusted exchange framework will address over time. However, the draft language implies selection is *limited* to these sources: *"Specifically, HINs should **first** look to use standards adopted by HHS, then those approved by ONC through the proposed standards version advancement process as part of the ONC Health IT Certification Program (Certification Program), and **finally,** those identified in the ISA"* (emphases ours). Innovation must be allowed to explore beyond these sources for applicability to the trusted exchange framework, or use cases that the trusted exchange framework is uniquely positioned to advance.

Lastly, we suggest that standardization also address testing tools. While the proposed QHINs may require specific/unique tooling given the scope of their capabilities beyond the core TEF capabilities, consistent expectations and validation of documents, APIs, and messages (for example) is critical; a number of the proposed and necessary standards will require consistency beyond the QHIN-QHIN focus. In particular, as outlined later, we should not assume nor prescribe that all data flows back-and-forth between Participant Members through a central QHIN server.

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

In general, the EHR Association supports the need for transparency. Also, we appreciate the notion of using arbitration processes, where reasonable and possible, to address challenges and differences in interpretations.

We note that not all matters are suitable to be made public, depending in part on the stage of a process, and we recommend providing adequate opportunities for parties to state their case, presuming good faith efforts until clearly demonstrated otherwise. Operating procedures should carefully consider these aspects when determining when and what can and should be made public, based upon this principle that transparency is critical to maintaining trust.

We appreciate that considerations around consent and authorization by the QHIN in this principle were moved in Draft 2 to more suitable sections, where we will provide further feedback.

While we support that terms, conditions, and contractual agreements are public, we do have concerns with what we understand to be an approach where new agreement language is being developed that effectively would create a parallel framework to what is already operational and expanding rapidly. We will provide further insight into our concerns in the MRTC section.

TEFCA requires HINs to provide a method for individuals to make a meaningful choice about their use and disclosure of their EHI data and to limit use to the minimum amount required for non-treatment purposes. Critical to adhering to and implementing these privacy practices is a well-defined common standard to capture and manage individuals' consent and authorization. Can TEFCA recommend/require the use of a specific consent standard, such as XACML or FHIR Consent Directive?

---

**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**

EHR Association members support this principle and suggest that all actors must be reciprocal in principle, with the exception where consumer-focused service providers may only perform queries, not necessarily reciprocate to queries from others, e.g., providers.

We note that MRTC 7.1 would need to recognize such a carve out. Consumer-focused service providers should not be prohibited from being accessible when the patient provides consent. It must be the patient's choice if they want to be reciprocal.

**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**

EHR Association members strongly support this principle to enable maintenance of protected and secure data access and exchange, in accordance with applicable privacy and consent policies under HIPAA or non-HIPAA use cases.

Patient matching across and within health IT systems is still a barrier to interoperability. The MRTC language on patient matching does not capture or recognize patient matching challenges such as ambiguous matches, multiple matches, and other issues that can cause a false positive match of patient records. Though the QTF does note additional requirements of a QHIN for patient matching, no solutions to the above issues are included. As patient matching is a patient safety issue, more technical information on how to perform and resolve patient matching challenges is needed.

We recognize the need to use certain demographic data to enhance record matching in the absence of stronger identifiers and improved registration processes and tools that improve data quality for 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 work closely with the healthcare community to establish minimum data set and standards, in order to avoid sending too much PHI for purposes of identification, which is a security risk in itself.

There are provisions within TEFCA for including a new security labeling requirement. If the patient data includes information that is labeled due to its sensitive nature—such as substance abuse, HIV, or mental health data—we believe that the exchange of such data should now require a higher degree of patient matching confidence. It is important to recognize that incorrect matching could cause a violation of privacy, which under 42 CFR is considered a felony.

We very much appreciate and support the ability to require non-covered entities to abide by the same privacy and security policies as covered entities, in order to protect PHI. We note that a trusted exchange framework can offer non-covered entities the opportunity to rapidly scale their connections to their customers' data holders, thus improving their value and service to consumers. That is possible due to sharing a common trust level. Those who believe it to be too high a bar still have the opportunity to pursue connections outside the trusted exchange framework, albeit perhaps at a slower pace. We encourage existing HINs to be confident to pursue participation by non-covered entities under this principle's guidance.

We appreciate the principle of meaningful choice and believe this concept is meant to be an all or nothing participation by a consumer/patient in a trusted exchange framework, while consent is another tool to refine data sharing when generally the consumer/patient opted-in. We suggest that this variance be further clarified to better understand the choices to be made. In particular, there must be clarity whether meaningful choice needs to be applied retroactively or only from that point forward, particularly if the choice is changed from sharing to not sharing. Once data has been documented and used in clinical decision making, it is very challenging to remove such data retroactively, as it may have been the basis for a critical decision that then would be subject to challenge without the evidence or inputs still available.

Therefore, we suggest that meaningful choice is active if changed from sharing to not sharing from that point forward, until changed, while a change of not sharing to sharing may be applied retroactively. Also, we note that any notion of the right to be forgotten, as is beginning to be discussed, be addressed completely separately, with caution surrounding similar considerations.

More detail about this consent piece would be helpful. In addition to a common standard for capturing and managing consent, it will be important to identify a common vocabulary for available options. For example, offering patients the option to state, "Only share in an emergency" rather than a binary "share" or "don't share." Without prescriptive details, systems may not be able to truly honor meaningful choice.

Lastly, we suggest that where law allows, the default is opt-in, as this has demonstrated to provide the greatest value to the most patients/consumers. We provide further feedback in the QTF on how such choice is best managed.

---

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

The EHR Association supports 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 part of USCDI—thus does not necessarily have the same level of interoperability standards and infrastructure in place, even though it is maintained in electronic form—may not yet 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 community to establish reasonable expectations and clarify what would be unnecessary in the context of then-current infrastructure and capabilities.

Also, we would like to see an exception made for information blocking for security reasons, as proposed in ONC's proposed rule on information blocking.

---

**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**

While EHR Association members support the need to enable population level bulk data exchange, we agree with the statements made on page 12 of Draft 2 that the capabilities to enable this are not sufficiently mature at this time to include in "phase I."

As indicated in the text on page 30, this is further acknowledged in the last paragraph. However, the combination of the second and third paragraph seems to imply that the exchange of population level data may be fully satisfied outside of the trusted exchange framework using APIs through mutual

contracts. If the intent is indeed to address fully outside of the trusted exchange framework, this principle is not relevant. However, we believe that certain aspects of population level data exchange can benefit from capabilities provided by a trusted exchange framework. Therefore, we suggest clarifying that such capabilities will be explored in future phases; thus, the principle is maintained and does not preclude the opportunity for improved scaling and access through a trusted exchange network.

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

### 1. Definitions

EHR Association members appreciate the general alignment of definitions between the MRTCs and the proposed definitions in the ONC Information Blocking and Certification proposed rule (and related proposed rules) and strongly support continued alignment.

We note that the focus of the EHI definition in TEFCA Draft 2 on, "*electronic protected health information, and any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in 'electronic media,'*" provides an ambiguous scope of the data. This definition, in particular the phrase *"any information that can be used to identify the individual,"* is subject to interpretation. We recognize the need for a neutral term that can work with covered entities and non-covered entities alike, but it should not vary in the specific data classes and associated data that are consistent and unambiguous. We recommend improved alignment with PHI/Designated Record Set data classes directly through the use of USCDI to create clarity and predictability.

Our specific comments on the scope of the Health Information Network state that they are overly broad. We suggest this be more specific to organizations that directly facilitate data access and exchange.

The difference between Meaningful Choice and Consent should be better defined, as both concepts are applicable between QHINs, to ensure that the right information is shared, or not shared, with the right person or organization.

---

### 2. Initial Application, Onboarding, Designation and Operation of QHINs

The EHR Association suggests that this entire section should be moved to the QTF to further disambiguate the questions about the architecture chosen, federated or centralized, or some mix thereof, for specific use cases and aspects of those use cases. Those are decisions and approaches that should not be made through MRTCs.

As highlighted in our response in the QTF, we suggest it be made clear that when referencing capabilities of a QHIN it be done relative to the QHIN in total, inclusive of its Participants and Participant Members, so there is no assumption of requiring a centralized QHIN server approach through which all data access and exchange is to physically flow.

**3. Data Quality and Minimum Necessary**

The EHR Association suggests that expectations on which party defines and manages data quality and minimum necessary criteria are not just the QHINs. Rather, responsibilities would vary based on the role of the QHIN (or its Participant or Participant Member) as either a sender/requester or responder in a particular use case. By particularly focusing on the sender (for message delivery) and requester (for queries) on minimum necessary, a trusted framework would ease the ability of responder to the query or the recipient of the message to better take on their responsibilities, while the responder to the query and sender of the message primarily focus on data quality. Further clarification and guidance is then to be provided through the QTF.

---

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

EHR Association members appreciate the clarification that breach notifications apply whether or not a QHIN is a covered entity, as well as addressing for the QHIN, Participant, and Participant Member.

We support the need to address patient consent and would like to reference our comments on the challenges with data segmentation and consent management in response to the ONC Information Blocking and Certification proposed rule.

We suggested in our response to the ONC Information Blocking and Certification NPRM that there are challenges with sufficient standards of privacy policies to security labeling that result in making the security labeling beyond the document level challenging, complex, and labor intensive. We agree that as clarity is gained on how to best manage security labeling and consent management within and across networks, the QTF is the most appropriate place to introduce the relevant standards and guidance identifying where consent information may be kept, how it is to be communicated, and at what level of granularity.

In that context, we suggest that the MRTCs not create a requirement on the QHIN that all consent processes and data storage must be done using centralized QHIN servers. That may be a configuration, but it may not be the only configuration enabling that capability. Therefore, we recommend that the text in sections 6, 7, and 8 apply to the extent the actor maintains and/or manages such data, where the QHIN must ensure the centralized or federated capabilities are in place to achieve the desired outcome.

We recognize that at this point the consent approaches between 42 CFR Part II and HIPAA vary and would like to express our continued interest that these be aligned to the extent possible by law, at a minimum using common vocabularies and labeling to maintain consistency. We appreciate, in that context, that the Common Agreement approach is not specific to either context, thus enabling the trusted exchange framework to support both contexts.

Draft 2 proposes to extend HIPAA privacy and security regulations to all TEFCA participants, even those who are not covered entities or business associates under that law, as necessary and welcome to maintain the privacy and security of EHI being exchanged. We support this extension to HIPAA for this use case, but what is the legal standing? As a voluntary agreement between participants, this proposal

may work to expand the security and privacy regulations of HIPAA to those who are not currently covered entities or business associates. We request clarity on how this will be enforced.

Additionally, we feel we need to understand further the actual security benefit of encrypting bearer authentication tokens, in addition to signing them, as required by FAL2. Encryption of the claims/assertions is useful if the token payload contains publicly identifying information, PHI or PII, but most authentication tokens do not contain this information. If the concern is the potential for an attacker to modify/tamper with the content of the token, this is already addressed by signing and the underlying secure transport channel (secured by TLS). It is important to consider how the token is presented to the relying party. For example, if the token is presented directly from the IdP to the RP, without going through the subscriber (or client), there may not be a need to encrypt the token.

We appreciate alignment of the trusted exchange framework with NIST standards and particularly those focused on risk-based processes and procedures within the MRTCs.

We support the intent of identity proofing. However, within the proposed standards and approaches, consistency of identity proofing is challenging; there is no provision for "certifying" identity proofers to the proposed NIST standards within the trusted exchange framework, in order to establish consistent trust in the identity proofing across the framework. Therefore, we suggest that for consumers/patients accessing their data that IAL2 be set as the target; but, for staff of QHIN and HINs (be they Participants or Participant Members) that current identity proofing to provide access to their HIT assets is appropriate.

An especially critical component of the entire system is that *"each QHIN who is an issuer of certificates shall maintain backup copies of system, databases, and private keys in order to rebuild the certificate authorities' capability in the event of software and/or data corruption."* We recommend that there be prescriptive requirements for strong security measures here. For example, using stringent guidelines such as those defined by DirectTrust.org—which governs direct messaging—for private key management.

---

**7. Participant Minimum Obligations**

Similar to our feedback to section 2.2.1, the EHR Association suggests Exchange Purposes and EHI Reciprocity is best addressed in the QTF.

Again, it is noted that if the participant is serving as a certificate authority that they should have *"Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption."* We believe more should be required to ensure data integrity; this is a critical component which needs to be especially secure.

We believe that future versions of TEFCA should expand upon the requirements for validating compliance of its participants, beyond voluntary written attestation.

**8. Participant Member Minimum Obligations**

Similar to our feedback to section 2.2.1, the EHR Association suggests Exchange Purposes and EHI Reciprocity is best addressed in the QTF.

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

EHR Association members appreciate and support the separation of the references to specific technology standards into a separate document, the QTF. In our review of the MRTC, we noted that we believe another section, addressing exchange modalities, would be better addressed through the QTF. The statements made in the MRTC imply a technical architectural approach where it appears to assume a central QHIN server to be the gateway/broker for any data that flows across QHIN boundaries. We believe that architectural choice is either not required, nor desirable based on specific use cases—or part of the use cases (e.g., endpoint discovery may be centralized, but for document exchange a brokered approach may suit better for actual query to that endpoint, while for FHIR based API access it goes directly from the client to the endpoint, not through a central server).

We understand and support the interpretation that the current version is very much a draft and is expected to be further fleshed out by the RCE once identified in close collaboration with (aspiring) QHINs, Participants, and Participant Members as appropriate. We suggest that the engagement be modeled after the way Carequality worked with representatives of its community, which was not limited to only those who had chosen to become a Carequality Implementer. Consequently, we strongly suggest that further development of the QTF not be based solely on comment/response and listening session approaches, but on guidance from workgroups that can collaborate on an ongoing basis. Such an approach has been very successful with eHealth Exchange, CommonWell, Carequality, and other collaborative initiatives of this nature.

We are concerned that the proposed approach will effectively result in a re-development/build of a technology framework in parallel to what is already in place and is successfully demonstrating that varied HIN approaches can access and exchange documents across those HINs. We are confident that this approach can progress those efforts into data element/set level access and exchange using FHIR based APIs and other appropriate technologies. Therefore, we strongly suggest that the QTF start with the Carequality technology framework and encourage participation to further evolve and mature these capabilities and develop the next set of capabilities.

For current capabilities, the focus should be on working with Carequality to identify opportunities to encourage those not yet participating directly, or through their Implementers, to join, addressing challenges in variances of supported purposes, data rights, etc. For new capabilities, the focus should be encouraging the industry to collaborate with Carequality, e.g., encourage FAST to work even more closely with Carequality to support their efforts to enable FHIR based API access rather than developing a separate set of guidance.

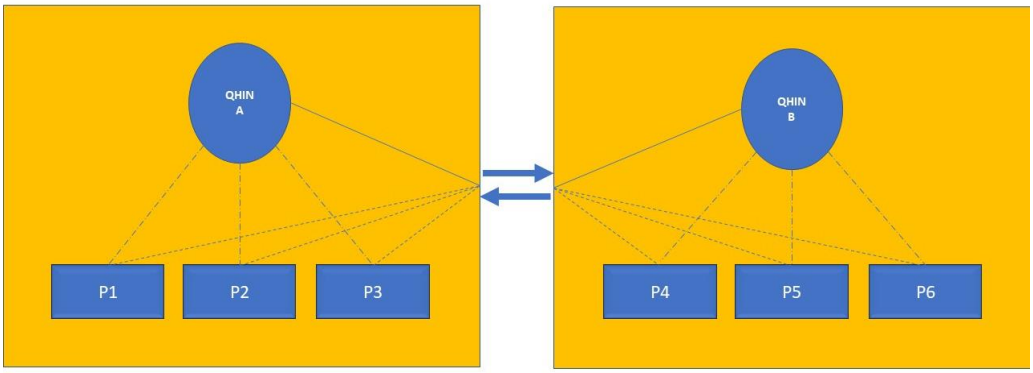
**1. Definitions**

With respect to the definitions, the EHR Association offers the following questions and considerations:

*First Degree Entity*
The scope of First Degree Entity suggests inclusion of individual users, yet does not mention Participant Members. We believe that First Degree Entities are primarily Participants (with their health IT suppliers if providers/payers) that interact with the QHINs, while Participant Members and Individual Users may as well interact with the QHINs, depending on how the QHIN operationalizes its various functions.

The latter goes to the question of whether the QHIN is perceived to provide for all data flows to go through a central QHIN server, or whether the QHIN is a black box to the other QHINs, thus may have certain traffic directed to decentralized/federated clients and servers. We suggest that this is a more practical view and ask that text in the QTF and diagrams in the User Guide clarify that any impression that all data must always flow through a central QHIN server is not assumed.

The following diagram would clarify this where traffic for certain use cases (or parts thereof and depending on whether endpoints and/or patients are already known, or whether it is a broadcast query or push, targeted query or push) could follow the dot-dash lines through the QHIN's central server, and/or a dashed line directly to one or more endpoints.




*Participant / Participant Member*
We note that accommodations should be made that there may be additional layers between the Participant as a First Degree Entity and a Participant Member where end users are serviced. We suggest the definitions should allow for multiple levels that must appropriately pass through the applicable terms, such as those in MRTC sections 7 and 8.

*QHIN*
There is ambiguity/inconsistency in text that on the one hand states, *"**Minimum Required Terms and Conditions (MRTCs):** ONC will develop the MRTCs, which will consist of mandatory minimum required terms and conditions with which Qualified Health Information Networks (QHINs) may voluntarily agree to comply."* On the other hand it states, *"A QHIN must meet the definition of a Health Information Network (HIN) and satisfy all of the conditions of the Common Agreement and accompanying QTF."*

We request that the "may" in the first statement be reconciled with the "must" in the second statement, as they seem to conflict. We note that this should be resolved in the context of earlier suggestions that the governance, legal, and technical frameworks build on what exists rather than establish a parallel framework.

*Patient Matching Data*
We note that in MRTC Section 3.1 there is a reference to "patient matching data," but there is no analogous language that operationalizes that in the QTF. We suggest adding a general definition for the concept of patient matching data that references the QTF where the then most current data set, formatting standards, and so on can be further defined. Also, provide guidance on when and how to use in the various use cases.

---

**2. Example QHIN Exchange Scenarios**

EHR Association members generally agree with the basic building blocks for the document exchange broadcast and targeted query technology framework. We have learned that the IHE profiles provide a good starting point, but still require further refinement and definition for a particular implementation.

Effectively, the proposed framework creates a new effort to redefine the necessary refinements to enable cross HINs. That work, as indicated earlier, has already occurred, thus we suggest continuing efforts based on where the industry is, rather than taking a step back and re-establishing that guidance. The focus should be on encouraging stakeholders to connect through the existing choices already available. As challenges come up, they can be resolved through the common framework already in place. ONC, in collaboration with other agencies, can provide substantial value by encouraging progress and participation.

Regarding the message delivery exchange modality, it is unclear why IHE XCDR was identified as the primary profile to enable this use case. We note that the Direct protocol has very wide adoption for direct messaging that can be used within, across, and outside networks, thus creating a much wider span to reach the intended stakeholders. We suggest that the RCE addresses this choice as part of its collaboration with (aspiring) QHINs, Participants, and Participant Members.

We recognize and agree that FHIR based APIs can provide an alternative mechanism to the IHE Document Exchange profiles to enable document exchange. Exploring APIs as an alternative is appropriate; we note various HINs are already actively pursuing that option for all or part of certain use cases. This should not be an immediate requirement, as the community may determine that pursuing data element/set level access and exchange using FHIR based APIs has a higher priority as the next step.

We would like to reinforce in this section that the internal approach of a QHIN to use centralized, brokered services—as currently implied (although perhaps not intended)—is not a requirement, thus different QHIN/HIN environments may opt to centralize/federate different aspects of the use case at hand. However, at whatever level endpoints are exposed for use of communication outside the QHINs environment, we agree that the standards used are those agreed to at the "QHIN level."

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

The EHR Association supports 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 exchange (e.g., document vs. data element/set). One should not assume a centralized QHIN server to be in place for all use cases or parts of use cases.

Consistent with our prior responses, we note that the Mutual QHIN Server Authentication approach should be agnostic to the actual clients or servers connected in the QHIN environment for cross-QHIN access/exchange.

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 state that there must be a commitment to maintain 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**

Regarding ***RfC #2,*** the EHR Association agrees that more specific guidance regarding User Authentication is required than provided in the current draft. We suggest starting with those referenced in the Carequality Query-Based Document Exchange Implementation Guide and evolve from there over time.

Regarding ***RfC #3,*** the EHR Association suggests considering the Carequality Query-Based Document Exchange Implementation Guide as a starting point for Authorization & Exchange Purpose. 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.

We appreciate that for document exchange the level of labeling continues to be at the document level. We refer to our comments to the ONC Information Blocking and Certification proposed rule where we outline deeper concerns and suggestions to consider alternate, more practical approaches. The current standard of standards and practice would create user mediated labeling that would likely yield inconsistent and inadequate labeling.

In various response letters and discussions, we have advocated for an opt-in approach as the default for meaningful choice and consent, particularly for TPO purposes. We recognize that for other purposes

default opt-in may not be appropriate. However, the vocabulary used to express/label data and consent should be consistent across purposes. As data is shared across covered and non-covered entities, there is consistency in clarity on what the data can or cannot be used for, including sharing with subsequent entities.

Regarding ***RfC #4,*** the EHR Association suggests 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 that wherever in its configuration this is identified, it is consistently and appropriately communicated to the other QHIN using "QHIN level" standards.

Regarding ***RfC #5,*** the EHR Association agrees 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. We recommend starting with the Carequality Query-Based Document Exchange Implementation Guide and building from there.

Regarding ***RfC #6,*** the EHR Association agrees 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. Also, this approach can consider the privacy concerns associated with expanding the document metadata content, with certain data that now will be further exposed.

We suggest that for Message Delivery, while XCDR works within networks or perhaps across networks, Direct can do that, plus connect anyone not in a network, thus enabling a wider range of interoperability. Consequently, we suggest that XCDR should be the extra, while Direct should be the main focus.

Regarding ***RfC #7,*** the EHR Association suggests starting with the Carequality Query-Based Document Exchange Implementation Guide for Patient Identity Resolution, while considering as well the EHR Association's feedback to both the ONC Information Blocking and Certification proposed rule and the CMS Patient Access and Interoperability proposed rule. In summary, 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*** and 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,*** the EHR Association suggests 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,*** the EHR Association suggests 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 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 is 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,*** the EHR Association supports 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,*** the EHR Association suggests that for 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 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.

Similar to the Patient Matching comment earlier, 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 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,*** the EHR Association acknowledges challenges with interstate QHIN communications

(whether within a QHIN spanning states or across QHIN spanning states). However 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, we reference our feedback on the ONC Information Blocking and Certification proposed rule related to data segmentation and consent. 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. Also, we 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,*** the EHR Association suggests that EHRs have robust audit capabilities. Their audit lists would serve as a solid starting point considering §170.210(h): Audit log content. 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 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,*** the EHR Association suggests that error messages should be specified by RCE in collaboration with the (aspiring) QHIN, Participant, and Participant Members as appropriate. Acknowledgement 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.