July 16, 2019
Donald Rucker, MD
National Coordinator for Health IT
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker,

The Health Information Technology Advisory Committee (HITAC) requested that the Trusted Exchange Framework and Common Agreement (TEFCA) Task Force (TF) provide recommendations to the HITAC regarding the proposals in the TEFCA Draft 2. This transmittal offers these recommendations, which are informed by the deliberations among the TF subject matter experts and the entire HITAC. The TEFCA TF and HITAC reviewed, discussed and approved these recommendations for transmittal at its July 11, 2019 meeting.

1. Background

1.1 Overarching charge: The Trusted Exchange Framework and Common Agreement (TEFCA) Task Force will develop and advance recommendations on the TEFCA Draft 2 to inform the development of the final Common Agreement.

1.2 Detailed charge: Make specific recommendations on the Minimum Required Terms and Conditions (MRTCs) and the Qualified Health Information Network (QHIN) Technical Framework (QTF).

- » **Definition, Structure, and Application Process for QHINs:** Recommendations for further clarifying the eligibility requirements and application process for becoming a QHIN.
- » **QHIN Technical Framework, Exchange Purposes and Modalities:** Recommendations on the overall functional requirements in the QTF. Recommendations on enhancing or clarifying the seven (7) exchange purposes and three (3) exchange modalities proposed in the MRTCs, as well as provisions regarding EHI reciprocity and permitted and future uses of EHI.
- » **Privacy:** Recommendations on privacy requirements for participating entities, including Meaningful Choice, Written Privacy Summary, Summary of Disclosures, and Breach Notifications
- » **Security:** Recommendations on security requirements for participating entities, including minimum security requirements, identity proofing, authorization, and authentication.

2. Overarching Recommendations

2.1 Value Proposition and Interoperability and Information Blocking

Recommendation 1: As part of our deliberations, the TEFCA TF discussed the overall value and purpose of the TEFCA, the incentives for participation, and what a successful TEFCA would look like. The TF also looked at the TEFCA in relation to the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program proposed rule (ONC Interoperability Rule) and framed two possible policy goals/views for consideration. The first, more narrow view considered whether the proposed TEFCA would address the means and intent of Congress with respect to providing an optimal path to "full network-to-network exchange of health information." The second, broader view considered whether the TEFCA as drafted expresses the broader policy aims and goals of improved care, improved health and reduced cost, and also whether it serves to reduce the prevalence and probability of information blocking without representing a safe harbor.

The TEFCA should express the broad policy aims of enabling better treatment, quality of care, and a more efficient health system. The TEFCA can only meaningfully advance these aims if it is:

- Carefully crafted to balance the addition of new requirements with complementing/coexisting with existing frameworks and networks, and
- Appropriately adopted by the stakeholders of health and healthcare that must exchange information.

We therefore recommend significant attention to both of these key issues:

Complement existing frameworks and networks – Consistent with the 21st Century Cures Act, TEFCA will best accomplish the above policy aims if its goal is broad, appropriate, secure, and seamless or low-friction exchange of health information with individuals and across the healthcare system. The TF believes it is important to view and leverage existing frameworks and networks as assets in achieving that aim and urges ONC to craft TEFCA with that view. In general, this implies that whenever possible the TEFCA should minimize any disruptive impact on existing frameworks and networks, without compromising the goals of TEFCA.

Incentivize Adoption of TEFCA –The second draft of TEFCA manifests that ONC has clearly listened and responded to feedback. The more the final TEFCA is artfully balanced to achieve its ends in a way that is accommodating for stakeholders, the more likely stakeholders will organically adopt and participate in the TEFCA. The TF urges consideration of this perspective as ONC weighs new feedback and considers options and compromises. Regardless of how well conceived the final TEFCA is there will need to be sufficient incentives to encourage participation.

We recommend that ONC consider both "carrots and sticks" for TEFCA adoption, such as:

- Education and outreach across the industry
- Outreach to existing frameworks and networks to coordinate launch and adoption efforts
- Funding aimed at any emerging financial obstacles for QHINs and Participants
- CMS encouraging TEFCA participation
- Federal agencies requiring TEFCA participation as a condition of contracts with federal agencies

Recommendation 2: The TF discussed the relationship between information blocking and the TEFCA. While there are many examples of access, exchange and use falling outside of the information flows intended for the TEFCA, good faith participation in the TEFCA should be an easy means for the Actors to comply with the relevant information blocking requirements and become the defacto path to exchanging EHI.

ONC should align TEFCA with the ONC Interoperability Rule:

- Key definitions such as HIE, HIN, and EHI should be the same across both rules.
- Active, good-faith participation in exchange provided through the TEFCA should address and be evidence for compliance with information blocking requirements relevant to cross-network exchange purposes, uses and modalities provided through TEFCA.
- Because TEFCA only addresses a portion of information exchange activities relevant to information blocking, TEFCA participation alone should not be made a formal exception to information blocking or create a safe harbor.
- Participation in TEFCA should not be a condition of maintenance and certification requirements for the information blocking condition as suggested in the ONC's proposed rule. It should however, be an easy and direct path to address relevant requirements. Standards relevant for QHINs, Participant, or Participant Members should be considered in future certification requirements.

Recommendation 3: Further, the TF believes there is an inconsistency between the requirements for a query response in the information blocking section of the ONC Interoperability Rule and the MRTCs. The ONC Interoperability Rule assumes all EHI is being exchanged, whereas the MRTCs require participating entities respond, at a minimum, with available EHI in accordance with the USCDI standard. The TF believes the lack of a standard for the exchange of all EHI beyond what is addressed in the USCDI and any real-world implementation of exchange of EHI (as it is presently defined in the proposed rule) is likely to be problematic. Improvements in the exchange of valuable, meaningful, and consumable information will be achieved most directly by defining exchange requirements in terms of USCDI and then expanding that standard data set as rapidly as is practical.

ONC should move forward with the requirement for data to be included in a query response as proposed in Draft 2, at a minimum, with the subset of EHI specified in the USCDI if the respondent has the data available, and focus on rapid yet prudent expansion of the USCDI standard.

2.2 Applicable Law

Recommendation 4: As part of our overarching discussions, the TEFCA TF discussed Applicable Law as it relates to the TEFCA and boundary conditions for when and to whom Applicable Law applies. The TF believes the TEFCA Draft 2 prudently and appropriately extends several specific HIPAA obligations to Participants and Participant Members who may not already be Covered Entities (CEs) or Business Associates (BAs). We strongly support that extension. Furthermore, we understand Draft 2 adds additional clarity and alignment specific to HIPAA obligations on Covered Entities (CEs) and Business

Associates (BAs) which would assist with TEFCA adoption, and believes there should be more clarity on when and how TEFCA creates new and additional obligations beyond those already under HIPAA.

The TF understands that Draft 2 creates new rights of individuals regarding access to their health information and calls out specific HIPAA obligations (such as 45 CFR 164.524) to explain these new rights. We also understand that existing HIPAA obligations to share information are not supplanted by these new rights. For example, HIPAA requires information to be shared with Public Health Authorities, and this information sharing is still required even after an individual exercises his or her right of Meaningful Choice to not have his or her EHI Used or Disclosed via the TEFCA.

To add clarity and avoid misinterpretation, ONC should categorize Privacy and Security obligations as:

- **HIPAA obligations extended to cover Participants and Participant Members who are not CEs or BAs.**
- **New privacy and security obligations which go beyond HIPAA and cover all Participants and Participant Members, such as:**
    - **Meaningful Choice**
    - **No EHI Outside the US**
    - **Specific identity-proofing and authentication policies (IAL2 and AAL2).**

Recommendation 5: To comply with MRTCs, existing Health Information Networks (HINs)/Health Information Exchanges (HIEs) will likely need to amend the terms and conditions in their participation agreements to enter into and sign the Common Agreement and participate in the QHIN Exchange Network, and those amended terms will flow down and impact Participant and Participant Member agreements as well for TEFCA-related activities. In order to minimize the disruption to existing networks, we recommend the MRTCs be addressable through terms and conditions in existing agreements whenever possible through such means as:

- Allowing the RCE to evaluate and approve a QHIN candidate's existing participation agreement or relevant terms of that agreement, with or without modification, as meeting the requirements of the MRTCs. In turn, allow QHINs, with the support of the RCE under a clear governance process established by the RCE, to evaluate and approve existing Participant agreements or relevant terms of those agreements.
- Designating TEFCA terms and conditions as "required" and "addressable."
- When changes to existing agreements are required, allowing Participants and QHINs to participate in TEFCA while having a defined period of time to revise their terms and conditions to avoid disruption to their participant network and existing information exchange. With respect to the RCE-QHIN relationship, the RCE may be able to employ this concept by appropriately grouping cohorts based on their bootstrap period/agreement.

3. Definition, Structure, and Application Process for QHINs

The TF supports ONC's proposal on the definition, structure, and application process for QHINs in TEFCA Draft 2 with no further edits.

4. QHIN Technical Framework (QTF, Exchange Modalities, Exchange Purposes)

Recommendation 6: The TEFCA TF discussed the proposed exchange purposes and modalities in the TEFCA and whether Draft 2 contains the right bundling of purposes and modalities. The TF deliberated the definitions of the exchange modalities and the functional requirements in the MRTCs, and discussed whether the technical and functional requirements in the QTF are responsive to the policy goals in the MRTCs. In general, the TF believes the ONC should focus on specifying policy and functional requirements and defer technical solutions to meet those requirements to the RCE.

The TF notes there are inconsistencies between the diagrams in the QTF and the definitions and functional requirements in the MRTCs. For example, Figure 1 on page 81 implies broadcast of a request received by a QHIN to "First Degree Entities." Depending on the deployment model by which a QHIN meets the functional requirements, the QHIN could respond directly via a record locator service or a document repository.

The TF discussed the challenges inherent in patient matching and linking. The functional requirements imply but do not mandate specific patient matching and linking approaches. We believe this is the right stance for ONC to take. At the same time, we encourage the ONC and the RCE to continue to monitor the state of the art with respect to patient matching and linking for those QHINs, which use patient matching and linking in their operations, as well as for participants and participant members.

The TEFCA should outline functional requirements sufficient to meet the policy goals in the TEFCA and avoid whenever possible identifying specific technical solutions. The QHIN functional requirements should be put front and center to communicate the "what" and leave room for flexibility and innovation on the "how." Because the RCE and initial QHINs are presumed to have familiarity with exchange standards and approaches, we recommend the ONC remove the QTF, and clearly document functional requirements (perhaps in a QHIN Functional Framework (QFF)). Given the QTF was created as initial guidance for the RCE, which has authority to work out flexible and evolving technical approaches with the QHIN Exchange Network, we recommend the RCE be provided the comments and feedback the ONC received in the comment period. We recommend it be clear the RCE is free to choose any technical enablement(s) of the functional requirements listed in the QFF.

Recommendation 7: The TF discussed the terms QHIN Targeted Query and QHIN Broadcast Query described in Draft 2. Our understanding of these terms as described is not the same as the generally understood industry terms "targeted query" and "broadcast query." As an example, our understanding is the TEFCA 2 functionally requires the QHIN to identify Participants, Participant Members, and relevant data, through means, which might include a document repository or a record locator service [RLS] to avoid large-scale proliferation of queries. The industry term, by contrast, implies targeted query to a single setting of care (Participants and Participant Members), and broadcast query to many settings of care. Reuse of terms in a different context will cause confusion.

We recommend the ONC focus on the functional requirements for QHIN query response, and avoid using the terms Targeted Query and Broadcast Query (or Record Locator Service), which have multiple interpretations/meanings.

Recommendation 8: The TF discussed the current requirement for QHINs, Participants, and Participant Members to satisfy all of the exchange modalities. While there is some elegance to the concept of a "single on-ramp," different exchange modalities require different capabilities and specialties.

All QHINs should serve a floor set of functional requirements, Exchange Purposes and modalities. Participants and Participant Members should be able to serve (and respond to) a subset of Exchange Purposes and modalities that are appropriate to their scenario of usage, constrained as appropriate by the needs of individuals as well as the goal of reciprocity.

Over time, QHINs and the TEFCA will evolve to add additional purposes and modalities above and beyond the minimum required, and we recommend flexibility to allow specialization for additional purposes and modalities.

Some of the core capabilities we expect all QHINs to offer are:

- Addressing the functional requirements for query
- Holding an individual's meaningful choice determinations and preferences
- Security standards
- Reciprocal exchange interaction with other QHINs
- Meeting the MRTCs

Recommendation 9: The TF discussed the goal of a "single on-ramp." As the TF noted in our previous recommendations, there are many nationwide exchange systems that are not well suited to the QHIN infrastructure requirements outlined by the requirements of TEFCA Draft 2. Examples may include electronic prescribing networks; HIN-mediated messaging, including ADT notifications; administrative networks; and the Direct ecosystem governed by DirectTrust. We believe such networks are parallel to the TEF and the exchange activities. All of these exchanges "deliver messages" on a nationwide basis.

While the TF understands the role that providing a common framework for query-based cross network exchange plays in national priorities, we were not clear on the role of Message Delivery in TEFCA Draft 2. We believe the goal is primarily to support public health reporting and other HIN-mediated messaging, but these goals are not clearly laid out in the TEFCA Draft 2.

ONC should clarify the role of the TEFCA relative to other nationwide exchanges served through parallel trust frameworks. In particular, ONC should clarify the intended uses of Message Delivery relative to other uses of network activities that send messages.

4.1 Individual Access Services (IAS)

Recommendation 10: The TF explored the definition and functional requirements of the Individual Access Services (IAS) Exchange Purpose. The TF strongly endorses the requirement for IAS, as well as the expansion of the HIPAA right to include all TEFCA participating entities. However, the TF notes that IAS is constrained to only two rights under HIPAA, 45 CFR 164.524—accessing and obtaining a copy of EHI and sending to a 3rd party. The TF discussed many other core use cases that could be valuable for patients but not included in the definition of IAS, including shared care planning, a patient's right to request corrections and amendments to their records under the HIPAA privacy rule, submit patient-generated health data (PGHD) and patient-reported outcomes, remote monitoring, and the Precision Medicine Initiative. The TF also noted that individual access rights have a different context for use than provider-to-provider exchange. As an example, while providers may need formatted clinical documents, individuals may be more likely to consume content on a mobile device with apps that more naturally fit discrete data API services. The TF was split on whether the IAS Exchange Purpose in the TEFCA should be expanded to include the full spectrum of individual needs up front, or whether such capabilities should be phased in by the RCE.

ONC should place the needs of individuals front and center in the TEFCA, and those needs will certainly be broader than exercising the HIPAA right to access over time, to include full access, exchange, and use. In addition, ONC should clarify the functional requirements for individual access, keeping in mind typical access patterns (for example, health app integration on a mobile device).

The Task Force proposed alternative recommendations for the initial extent of IAS.

Alternative Recommendation 10a: ONC should expand the IAS Exchange Purpose immediately to build in broader functionality for individuals that is not limited to obtaining and accessing a copy of their EHI, and sending to a 3rd party. At a minimum IAS should include the right for an individual to request an amendment to their EHI, as defined in HIPAA 45 CFR 164.526. Additional use cases to incorporate include:

- The ability for providers, patients, and payers to participate in shared care planning and to share and retrieve a patient's dynamic shared care plan for purposes of coordinating care.
- EHI that is created by or recorded by the patient, i.e. PGHD, patient-reported outcomes, and remote monitoring.
- The Precision Medicine Initiative led by the National Institutes of Health (NIH).

Alternative Recommendation 10b: ONC should establish a policy framework to get to broader individual services, including amendment, shared care planning, PGHD and data donation for research with a clear timetable. ONC and the RCE should roll out individual services that are ready for large scale adoption, starting immediately with IAS Exchange Purposes as described in Draft 2 as this constitutes a significant step forward for patient access. ONC should work with the RCEs and QHINs to develop and test the additional forms of individual exchange within the timeline established for the expanded usage.

Recommendation 11: The TF also discussed the definition of Direct Relationship and various scenarios for who is required to respond to queries for IAS. Specifically, the TF discussed the apparent requirement, as currently drafted in the MRTCs, for public health agencies to respond to IAS. In addition, the TF noted an inconsistency in the Draft MRTCs regarding whether all participating entities must respond to requests or only those with a Direct Relationship with the individual established by mutual agreement who is the subject of the information.

ONC should clarify whether all participating entities must respond to requests for IAS or only those with a Direct Relationship to the individual.

Recommendation 12: ONC should further clarify the meaning of the term Direct Relationship. The MRTC uses this term variously to refer to an individual's designated Participant(s)/Participant Member(s) that are allowed to initiate queries on the individual's behalf, and the relationships to recipients of such queries. For purposes of clarity, ONC should define a clear term (one that does not overlap with existing legal terms regarding treatment relationships), such as Individual Designated Participant/Participant Member, to cover the former definition.

For the latter definition, ONC should include relationships defined by Applicable Law in the definition. Further, the definition of Direct Relationship should detail the types of services that must be offered in order to establish a Direct Relationship.

Recommendation 13: The TF discussed the consequences of requiring all Participants and Participant Members to respond to all exchange modalities and exchange purposes. As an example, public health agencies that conduct surveillance activities (reportable diseases, reportable labs, etc.) may receive EHI, but maintain data for the purposes of aggregation and signal detection. Requiring these agencies to respond to queries, including for IAS, forces them to index and maintain patient-specific information that is outside of their mission and mandate.

The TF discussed the rare cases where public health agencies do maintain patient-specific information (for example, immunization registries and infectious disease case management), where expanded access to query, including for IAS, would be helpful but may be outside of the public health mission and mandate, without reaching a definitive conclusion.

ONC should not require all public health agencies to respond to query, including IAS, particularly those that primarily exist for disease surveillance and do not maintain a longitudinal patient record, except when it is required by Applicable Law (such as when a public health agency is acting as a CE under the HIPAA rules).

5. Privacy

5.1 Meaningful Choice

Recommendation 14: The TEFCA TF discussed the Meaningful Choice policy in the MRTCs, including its scope and intent. The TF thinks that the definition and scope of Meaningful Choice are not sufficiently clear about what the individual is choosing. We believe that clarity around this issue is especially important to maintain patients' trust and understanding. We note that Meaningful Choice, as drafted, is all or nothing and does not allow for exceptions for things like emergency treatment or more granular consent. In addition, there is concern that, as drafted, this is an underspecified set of requirements with many complications. Currently, there is no implemented technical solution for sharing the privacy preferences of an Individual's meaningful choice action across a network.

The TF also discussed the original intent of Meaningful Choice as a concept. The notion of Meaningful Choice was introduced to move away from the notion of opt-in and opt-out as the only two options. Opt-in and opt-out can be implemented in ways that fail to permit the patient to give meaningful consent. Rather, meaningful consent occurs when the patient makes an informed decision and the choice is properly recorded and maintained.

ONC should clarify the language and policy goals around Meaningful Choice and leave the granular technical requirements to the RCE. The TF recommends clearer definition of "Meaningful Choice" and its scope, to express (a) ONC's intent that, by default, Individuals' EHI is used and disclosed in exchanges under TEFCA unless the Individual exercises a Meaningful Choice to disallow any further, prospective Use and Disclosure, and (b) that, like TEFCA, the Individual's Meaningful Choice only applies to revoke prospective Use and Disclosure in exchanges within TEFCA but not use and disclosure of EHI outside of TEFCA. Policy goals should ensure that Meaningful Choice is not just a "check-the-box" exercise, but that it provides meaningful information and opportunity for discussion about where and how an individual's EHI will be used and disclosed. Consent should be meaningful in that it does the following:[1] (Note: The current definition of Meaningful Choice already captures the first, second, and sixth bullets below, but we include them here to complete the list.)

- Allows the individual advanced knowledge/time to make a decision. (*e.g.*, outside of the urgent need for care.)
- Is not compelled, and is not used for discriminatory purposes. (*e.g*., consent to participate in a centralized HIO model or a federated HIO model is not a condition of receiving necessary medical services.)
- Provides full transparency and education. (*i.e*., the individual gets a clear explanation of the choice and its consequences, in consumer-friendly language that is conspicuous at the decision-making moment.)
- Is commensurate with the circumstances. (*i.e*., the more sensitive, personally exposing, or inscrutable the EHI, the more specific the consent mechanism. Activities that depart significantly from a patient's reasonable expectations require greater degree of education, more time to make a decision, additional opportunity to discuss with his/her provider, etc.)
- Must be consistent with reasonable patient expectations for privacy, health, and safety; and
- Must be revocable. *(i.e*., patients should have the ability to revoke their Meaningful Choice and resume use and disclosure of their EHI under TEFCA at any time. It should be clearly explained whether such changes can apply retroactively to data copies already exchanged, or whether they apply only "going forward.")

Recommendation 15: Furthermore, the TF discussed the meaning of "prospective" as it relates to Meaningful Choice. As drafted, in section 2.2.3, an individual's Meaningful Choice must be respected on a prospective basis, but any EHI that has been used or disclosed prior to the Individual's exercise of Meaningful Choice may continue to be used or disclosed for Exchange Purposes. While we understand ONC's intent for allowing the continued use and disclosure of EHI that has already been shared prior to the exercise of Meaningful Choice, some members of the TF believe that this is problematic. The TF acknowledges the practical realities and issues with deleting the EHI once it has been incorporated into the patient records, but some members advocate for a recommendation that the EHI no longer be used or disclosed after an individual's exercise of Meaningful Choice. However, in general, once providers have incorporated data from the outside world into their patients' EHRs, the expectation is they will

[1] Health IT Policy Committee, Privacy & Security Tiger Team. September 1, 2010. https://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf

keep that information as part of the legal record because they will have used it to make treatment decisions.

It is reasonable and practical to permit the use and disclosure of an individual's previously-disclosed EHI following an individual's exercise of Meaningful Choice to not have their EHI shared through the TEFCA in light of the significant challenge created in contemplating how to implement applying such a policy retrospectively.

There was a very strongly held minority opinion that the TEFCA should expand the scope of Meaningful Choice to include restrictions on re-disclosure of exchanged information that has been obtained via the QHIN Network.

Recommendation 16: As drafted, once an individual exercises his or her Meaningful Choice to not have his or her EHI used and disclosed via the TEFCA, TEFCA 2 constrains the prospective use and disclosure of an individual's data to Exchange Purposes whereas prior to the exercise of Meaningful Choice, the use and disclosure was defined by Section 2.2.2 of the MRTCs. To avoid introducing unnecessary complexity, the TF recommends that the prospective use and disclosure of an individual's information after the exercise of Meaningful Choice continue to be defined and constrained by Section 2.2.2 and not the narrower Exchange Purposes only.

Recommendation 17: **ONC should clarify how broadly an expressed Meaningful Choice will be applied. Specifically, once exercised by an individual, the Meaningful Choice is expected to be communicated "up" the QHIN branch and shared by the QHIN with the other QHINs. Clarify which organizations in the TEFCA ecosystem are expected to be aware of that individual's Meaningful Choice and respect it. Also, clarify whether it is 1) only the organization with the Direct Relationship, 2) all Participants or Participant Members under that QHIN branch where the individual has a Direct Relationship, or 3) all QHINs, Participants, and Participant Members across the TEFCA ecosystem.**

5.2 Summary of Disclosures and Auditable Events

Recommendation 18: The TEFCA TF discussed the MRTCs provision around summary of Disclosures in connection with the provision on auditable events and agreed they should be discussed in parallel.

ONC should align requirements around auditable events and summary of Disclosures. The MRTCs should describe the policy requirements for audit retention, including what's required to be audited and how long it should be maintained, in the MRTCs and not delegate to the QTF. ONC should move the six-year retention requirement to the audit language.

Recommendation 19: The TF sought clarification on whether the summary of disclosures applies only to the entity with the Direct Relationship to the requesting Individual or to all of the other QHINs, Participants, and Participant Members in the network that have received and re-disclosed the Individual's EHI. It was noted that requesting the summary of Disclosures from everyone in the network would be very complicated.

The MRTCs should require a summary of disclosures only from the entity with the Direct Relationship to the requesting Individual (and the associated QHIN). Such a summary should include disclosures

when data have been pulled from the associated QHIN and disclosures when data have been requested by the associated QHIN.

6. Security

6.1 No EHI Used or Disclosed Outside the US

Recommendation 20: The MRTCs include a provision prohibiting QHINs from using or disclosing EHI outside of the United States except to the extent that it is required by an Individual or Applicable Law. Further, QHINs may only use cloud-based services that are physically located in the US. The TF agreed that the intent of this provision seems reasonable, but the TF thinks the language as written is too broad and ambiguous. The TF is concerned that there are valid use cases for which the MRTCs should allow for access to data in another country. For example, if a QHIN technical support person is traveling to another country, he or she would not be able to assist with technical support from that location but should be able to do so. The TF also raises for consideration the question of whether the Common Agreement would ever want to be used to exchange data with other countries, like Canada or Mexico. Many health systems in the US have locations in Canada and it would be unfortunate to categorically prohibit such exchange.

Further, the TF wishes to point out that security risks to data are so much greater and more diverse than just where the data physically reside. Most data do not live in one place and are replicated in many different places for backup purposes and charting. Focusing on where the data live does not lead to the best approach to regulating the security of the data. What matters is the proper safeguarding of network protocols and security protocols that govern network access.

ONC should focus on the need for risk-based security assessment and remediation for QHINs, and not make "where the data resides" the central criterion for security.

Recommendation 21: In order to clarify governing law, the restriction to have QHINs maintain data center operations and data at rest in the US is reasonable. ONC should define these requirements in terms of operations and data at rest, and not use the term "cloud services," which excludes on premise data center services.

Recommendation 22: Because of the need to have data follow the patient and because of the existence of international settings of care (e.g., Department of Defense Military Treatment Facilities), ONC should not restrict data access and exchange to US national boundaries and permit international data access and exchange.

6.2 Controlled Unclassified Information (CUI)

Recommendation 23: The TF discussed CUI handling with respect to EHI. The TF is concerned, based on past experience with Federal partners, that the net effect of CUI rules will be to create broad burden on prospective QHINs without meeting all the requirements of specific Federal entities. Instead, the TF believes that Federal partners and their chosen QHINs should bear the burden of Federal information handling rules. In addition, the TF discussed the importance of reciprocity – differing security requirements should not create a "two-tier" network or lead Federal partners to receive data but not provide data when permissible by law.

The TF recommends that ONC remove the section related to CUI.

Recommendation 24: The TF recommends that ONC make it clear that the additional obligations on CUI handling or other specific requirements will be borne by Federal partners. As Federal partners onboard to TEFCA-administered exchange, ONC should work with Federal partners to ensure additional security requirements do not impede the principle of reciprocity.

6.3 Privacy/Security Labeling

Recommendation 25: The TF discussed the goals of the security tagging request for information in the TEFCA. The TF believes that any security labeling policy should address three things: 1. How you apply the label; 2. What you do when you receive the document with the label; and 3. the governance behind it. The TF thinks provenance tracking needs to be solved first, before layering on complex behaviors related to security. There is still too much uncertainty around standards in this area and more work needs to be done before meaningful tagging can occur.

ONC should add Privacy/Security labeling to the TEFCA only via a common standards and policy framework that is implemented in provider workflow systems. As the HITAC recommended previously to ONC, there would be value to this proposal but more work is required to make labeling implementable. In particular, there should be accompanying policy guidance for how to handle labeled data. In particular, the policy framework should address when labelled data can and cannot be used, and how duplicate data that is labelled and un-labelled should be handled.

6.4 Certificate Authority Back-Up and Recovery

Recommendation 26: The TF believes the ONC should not include Certificate Authority (CA) services as part of the MRTC. The TF notes the requirements to be a trusted CA go far beyond the proposed MRTC terms and should be considered out of scope for TEFCA.

We recommend that ONC delete this provision.

6.5 Identity Proofing and Authentication

Recommendation 27: The TF discussed the proposed levels for identity proofing and authentication in the MRTCs. Based on past recommendations and current practices most members agree the levels suggested are appropriate. However, some members note the industry may require time to accommodate these requirements. The TF notes it expects to see a fair amount of technology and process change in this area over the next few years. Requiring two-factor authentication without specifying the specific technology used is therefore a reasonable approach.

For purposes of clarity, the TF recommends the ONC overtly state that QHINs can accept the identity proofing of Participants and Participant Members under its QHIN branch on the basis that all Participants and Participant Members have agreed to flow-down agreement terms specifying the same identity proofing standards as in the Common Agreement.

Recommendation 28: We agree with ONC's inclusion of AAL2 and IAL2. We recommend the ONC allow appropriate time for industry to accommodate these requirements.

The HITAC is supportive of TEFCA Draft 2 and offers these recommendations to improve the next TEFCA version. Please let us know if we can provide more information.

Respectfully submitted,

Carolyn Petersen	Robert Wah, MD
/s/ Carolyn Petersen Co-chair, Health Information Technology Advisory Committee	/s/ Robert Wah Co-chair, Health Information Technology Advisory Committee