



TEFCA Comment Letter

February 20, 2018

February 20, 2018

Dr. Donald Rucker, M.D.
National Coordinator for Health Information Technology
Office of the National Coordinator (ONC)
U.S. Department of Health and Human Services
330 C St. SW., Mary Switzer Building, Office 7009A
Washington, DC 20201

RE: Comments on the ONC Draft Trusted Exchange Framework and Common Agreement and Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process

Dear Dr. Rucker:

The Digital Bridge governance body is pleased to submit the following comments regarding the Office of the National Coordinator's (ONC) Draft Trusted Exchange Framework and Common Agreement (TEFCA) and Draft U.S. Core Data for Interoperability (USCDI) published January 5, 2018.

A first of its kind partnership, Digital Bridge ensures the health of our nation by establishing effective bidirectional data exchange between health care and public health. It creates a forum for key stakeholders in health care, public health and health IT to discuss the challenges of information sharing and implement multi-jurisdictional solutions. Through this collaboration, Digital Bridge fosters a better connection between health care and public health, a relationship that is integral to efficient public health surveillance.

As its first project, the Digital Bridge collaborative has designed a multi-jurisdictional approach to electronic case reporting (eCR). eCR is a valuable tool that reduces the burden of public health reporting of infectious diseases while improving the timeliness, accuracy and completeness of the data. Early detection of cases allows for earlier intervention, diminished transmission of disease and improved detection of outbreaks.

We commend ONC's efforts to advance nationwide interoperability by developing a trusted exchange framework that enables the seamless flow of health data between health information networks (HINs). Significant work has already been done in the private sector—as well as at the federal, state and local government levels—to establish health information exchange networks and support access to and exchange of health information in a secure manner. However, these networks continue to be challenged by the limited interconnectivity and interoperability that exist between them, leaving network participants with the inability to reach participants from other networks. These limitations also perpetuate the need for participants to connect to and transact data with two or more of these networks to access and exchange their members' and patients' health information.

We applaud ONC's recognition of public health as a permitted purpose in health information exchange. We understand from ONC that the benefit of TEFCA for public health agencies will be drawn from the

additional data made accessible via the trusted networks, allowing them to improve electronic case reporting, cross-jurisdictional immunization exchange, patient tracking and family reunification during emergencies, identification of at-risk populations, disease surveillance and outbreak investigation.

We also commend ONC's efforts to identify, specify and define a common set of data classes (to be known as the U.S. Core Data for Interoperability) that are required for interoperable exchange of health information and identifying a predictable, transparent and collaborative process for evaluating and expanding such a data set to achieve the goals set forth in the 21st Century Cures Act of 2016.

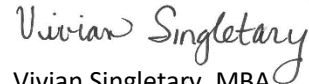
The comments we offer in this document are organized into three major parts:

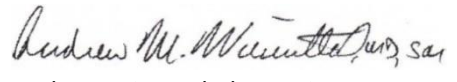
- Part 1: Overall Comments and Principles for Trusted Exchange
- Part 2: Comments on Minimum Required Terms and Conditions for Trusted Exchange
- Part 3: Comments on the USCDI

In each of these three sections we provide a series of overall comments followed by detailed comments on all the sub-sections.

We appreciate the opportunity to provide these comments on behalf of the Digital Bridge governance body. Please send any questions or concerns to info@digitalbridge.us.

Sincerely,


Vivian Singletary, MBA
Public Health Informatics Institute
Co-Principal Investigator, Digital Bridge


Andrew Wiesenthal, MD, SM
Deloitte Consulting, LLP
Co-Principal Investigator, Digital Bridge

Part 1: Overall Comments and Principles for Trusted Exchange

Overall Comments

We support the concept of TEFCAs as a network-of-networks framework and agreement, intended to foster and facilitate data flow from one end node to another across multiple health information networks (HIN). Such a framework will support data exchange whether the data flows between providers, between providers and payers, or between providers, payers and government entities, including public health.

We also support the model envisioned by ONC in TEFCAs that an end node or participating entity, such as a public health agency, would need to connect only to one qualified health information network (QHIN), and that through the network-of-networks interconnectivity and interoperability, the public health agency will be able to reach and communicate with all other organizations, whether they are connected to the same QHIN or not.

In today's flow of information, entities use a variety of mechanisms, including sending a query and receiving a response about an individual or a group of individuals ("query/response"); receiving data via a submission initiated and originated by a sender ("push" that is "unsolicited"); retrieving the data by going into a source system ("pull"); or accessing the data at the source system without extracting/retrieving it from the source ("real-time shared access"). While the TEFCAs are intended to cover all forms of data flows, we are concerned that TEFCAs are currently framed to only consider the query/response model and does not consider other models such as sending data (without query). While the query/response model suits certain data exchange needs (e.g., obtaining individual health records in support of care), it is estimated that over 95 percent of public health data exchange occurs via a submission of data initiated by the sender, and not involving an in-bound query. This is not a semantic difference but one that is derived from the role, authorities and workflows established in the clinical care–public health relationship. We believe it is critically important that TEFCAs, to the extent possible under applicable law, explicitly consider and support all these models, especially the "push" or sending mode that is critical to the ongoing operation of public health functions.

Patients and consumers are not critical, active participants today in existing HINs. They generally access their health information directly from the health care provider and health plan organizations that hold their information. TEFCAs seem to envision a framework where consumers and patients will be active participants in HINs, using them to access their health information from different sources. This will require a fundamental transformation in the way current HINs operate and require them to establish consumer-facing interfaces, policies and procedures not currently in existence.

Public health agencies are active participants in several HINs today and use them to exchange health information with various organizations, primarily health care providers. We are concerned, however, that very few specific public health data exchange transactions are supported by the architecture described in TEFCAs.

- As noted above, most public health data exchanges are done through provider-initiated reporting ('unsolicited', or not connected to a specific in-bound query message) using standards such as HL7 v2 messaging that currently support immunization data submission and electronic lab reporting. Other systems, such as vital statistics, also use provider-initiated electronic standard messages. Many health and disease registries use HL7 CDA standards to receive data from providers. Public health case reporting

(notifiable events and conditions) also use electronic standards and are gearing-up for the newest HL7 electronic initial case reporting (eICR) and reportability response standards.

- Queries to public health systems are generally executed by known (in many cases registered) end points using electronic interfaces specifically designed for such purpose.
- While many of these interactions occur within a defined jurisdiction, in many cases the two participants (provider, public health agency) are not connected to the same HIN, requiring that they either use secure public connections or point-to-point connections, or participate in multiple HINs. This is particularly significant when there is cross-jurisdictional reporting and information exchange.

TEFCA and HIPAA

We agree with the premise that throughout existing (and new) HINs, there will be a mixture of covered entities, business associates of covered entities, and non-covered entities. We are concerned, however, that the TEFCA seems to primarily reference individual consumers and patients when discussing non-covered entities. We believe there will be many different types of non-covered entities and individuals expected to participate in HINs.

- Individual patients and consumers participating in the HIN seeking access to their health information, among other things. As noted above, this will result in a critically important transformation on how HINs operate today.
- Non-individual patient/consumer, non-covered entities, and non-business associate organizations, such as independent developers/vendors/suppliers of medical/health apps, mobile devices, data brokers, etc., that will be seeking to obtain access to health information on behalf of the individual/patient. The main concern is the limited control that currently exists on these organizations once they have obtained the data.
- Public health agencies, which operate under specific jurisdictional mandate or direction to receive health information necessary to support the performance of their public health functions. We believe TEFCA does support the flow of information for this purpose.

The document states that "... we anticipate that many end users may not be Covered Entities or Business Associates as defined by HIPAA, and the final TEFCA must be broad enough to enable them to appropriately and securely access health information. Therefore, while the proposed Trusted Exchange Framework aligns with HIPAA requirements, it also specifies terms and conditions to enable broader exchange of health information..." The statement gives the impression that the only activity that non-covered entities will perform while participating in an HIE will be to "... appropriately and securely access health information..." This works well with patients and consumers accessing their own health information; however, there will be non-covered entities that are not patients and that will seek to access, receive, use and disclose health information. These entities will be able to do so outside of the HIPAA realm.

While the trusted exchange framework highlights the importance of privacy and consent as one of the core principles, the common agreement section of the document seems to pay little specific attention to the reality of inconsistent state, local and tribal patient consent and data sharing laws that are often an obstacle to cross-jurisdiction interoperability.

One complexity lies in data that are accessed. HIPAA—and at times state, local and tribal laws—limit the data that public health agencies can access. Under HIPAA’s “minimum necessary” provision, public health should only receive data necessary to meet a specific purpose. It should be clarified in TEFCa and in the U.S. Core Data for Interoperability (USCDI) that only necessary USCDI data should be shared for some purposes.

An “On-Ramp” to Data Liquidity

The document correctly specifies that “... At this time, a single network is not feasible, since there are technical limitations, security concerns, variations in the participants being served in use cases, and resource limitations for each network.” The document then makes the argument that “... However, establishing a single “on-ramp” to Electronic Health Information (EHI) that works regardless of one’s chosen network is feasible and achievable...”

We generally agree with the expectation that a single organization must choose only one “on-ramp.” However, we are concerned that this statement seems to imply that there will be one and only one “on-ramp” that everyone will use, when in reality there will be many on-ramps that entities and individuals will be able to choose from to avoid bottleneck. They will only need to choose one on-ramp, with the expectation that through that one on-ramp they will be able to access the data from all other end-nodes in all other networks interconnected through the network-of-networks framework. However, the document continues to emphasize in other places this concept of a ‘single on-ramp’: “...our goal is to use the successes in the industry to create the *single on-ramp*...” It will be very important that the document correct this misconception.

How Will it all Work?

According to TEFCa, ONC is intending to identify, select and contract with a single national Recognized Coordinating Entity (RCE) that will deploy, coordinate, operate, monitor and enforce TEFCa. While we acknowledge the value of having a single entity centrally oversee the deployment of the TEFCa, we are concerned about the level of national control and authority this single entity will have to 1) develop and establish the requirements of a single Common Agreement; 2) operationalize the Trusted Exchange Framework; and 3) monitor and enforce the voluntary adoption and abiding by the agreement from all QHINs. The level of control allocated to this central operator seems unnecessary and unparalleled in other sectors where a network-of-networks approach is used (such as banking).

Another example of the power that an RCE would be able to exert is illustrated by the statement “...To operationalize the Trusted Exchange Framework, the RCE will incorporate additional, necessary provisions into the Common Agreement as long as such provisions do not conflict with the Trusted Exchange Framework, as approved by ONC...” Yet another example of this concerning power can be derived from the following statement: “The RCE will be expected to monitor Qualified HINs compliance with the Common Agreement and take actions to address any nonconformity with the Common Agreement—including the removal of a Qualified HIN from the Common Agreement and subsequent reporting of its removal to ONC...”

An alternative, more feasible, public-private model and approach would be to consider (1) establishing an RCE with limited control and authority; (2) identifying and recognizing a handful of national-level entities (QHINs), all of which will offer “on-ramps” for HINs; (3) having regional and local HINs connect to a QHIN (a regional or local HIN would only need to connect to one of these national QHINs); (4) have end nodes or participants connected to HINs

(will only need to connect to a single HIN via the HIN 'on-ramp'); and (5) all three levels (QHINs, HINs, end nodes) will interconnect and interoperate among themselves with a TEFCA-based framework, operationalized by the QHINs, with the facilitating role of an RCE.

Comments on Principles for Trusted Exchange

1. Principle 1: Standards
 - We agree with the intent of requiring the use of nationally- (and internationally) recognized standards. We also agree with the need for everyone to adhere to standards adopted by HHS.
 - We are concerned with requiring adherence with standards "... identified by ONC in the Interoperability Standards Advisory...", as many of those standards are in various stages of development and maturity.
 - We strongly support the addition of "push" services, as a query model is not appropriate for numerous types of public health reporting.
 - We encourage the development and use of unambiguous implementation guides to support standards adherence.
2. Principle 2: Transparency
 - We agree with this principle.
 - We recommend that TEFCA should explicitly encourage the exchange of specific public health information to prevent silos from emerging.
3. Principle 3: Cooperation and Non-Discrimination
 - We are concerned that the increased expectations of services provided by QHINs in TEFCA will result in high costs for the QHIN and, in turn, high charges to end nodes/participants, potentially making participation cost-prohibited and hindering the flow of health data.
4. Principle 4: Privacy, Security and Safety
 - While we generally agree with the statements provided under this principle, this section focuses primarily on HIPAA security and there is no mention of privacy. There is also no mention of security and safety expectations of non-covered entities that receive, maintain, access, use or disclose data through the HIN and QHIN.
 - We are also concerned that there is no mention of cybersecurity protections by QHINs. In fact, in the entire document, cybersecurity is only mentioned twice as a reference.
5. Principle 5: Access
 - We are concerned that this principle seems to apply more specifically to the end nodes/participants in HINs, rather than to QHINs (unless the QHIN is maintaining patient-level data and is part of a business associate agreement to provide direct access to consumers, which would be very challenging).
 - While we support the statement regarding having "... policies and procedures in place to allow a patient to withdraw or revoke his or her participation in the Qualified HIN...", we are concerned this may not be clearly defined and might be problematic to execute. First, what does the statement "patient participation" in the QHIN mean? Secondly, does this extend to the patient being able to withdraw from having his/her data exchanged via the HIN/QHIN? Again, this will be very difficult to implement.
6. Principle 6: Data Driven Accountability

- We generally agree with this principle. However, we are concerned about (1) the capability of systems to perform standardized queries of population-level data and receive a response back; and (2) minimum necessary requirements that limit the amount of information to be disclosed.

Part 2: Comments on Minimum Required Terms and Conditions for Trusted Exchange

Overall Comments

We commend ONC's effort to define, in specific detail, the more than 120 different minimum terms and conditions expected to be in place and required of all participants (QHINs, HINs, End Nodes) who agree to abide by the TEFCA. We are concerned, however, that such detail is in many cases too prescriptive, overly complex, unnecessary, duplicative of existing terms and conditions, restrictive, limited in its ability to incorporate innovation, and over-reaching beyond the main goals of a true network-of-networks approach. We recommend re-evaluating each of the terms and conditions and considering offering many of them as templates for the QHINs to use in their agreements, but not as required components.

In many instances it is not clear whether a requirement, term, or condition applies to a QHIN only, or extends to the HINs connected to a QHIN or even to the end-nodes or participants in a HIN. Each of the elements should note to whom it applies. ONC should also consider whether any of the terms and conditions must directly apply below QHINs to HINs and even to end-nodes, as this could potentially open the door for establishing highly complex, expensive requirements that will make participation difficult for many organizations, both from a technical and monetary perspective.

The document states that each participant and end user shall support all of the permitted purposes and provide all of the data classes when requested and permitted by applicable law. We are very concerned about these provisions, as not all permitted purposes apply to all participants and all end users. This is particularly true for public health agencies and exchanges done for public health purposes. We recommend that ONC clarify this point and consider allowing entities to support the permitted purposes that are applicable to them. We further recommend that participants and end users (such as public health agencies, the Social Security Administration, etc.) that are participating in health information exchange for a limited purpose are not required to support permitted purposes that do not apply to them. We encourage ONC to structure the entire framework to offer the flexibility of a phased approach and modular implementation for all permitted purposes and data types opposed to an "all-or-nothing" approach.

As noted above, the overall TEFCA document centers around a query/response approach and does not consider other models, such as electronic data submissions initiated by a sender ("push"), data retrievals by going into a source system ("pull"), or accessing data at a source system without extracting/retrieving it ("real-time shared access"). In this section of the document, most of the detailed terms and conditions apply to a model that uses a record locator service, some level of individual identifier within HINs, and patient matching mechanisms to assert identity.

The document also seems to reference exclusively the HL7 Consolidated Clinical Document Architecture (C-CDA) as the standard for exchanging clinical information and ignores other data exchange formats, including HL7 V2 (2.x) messaging standards that today still account for a significant amount of exchanges, particularly with public health.

The document also briefly mentions newer standard approaches, such as HL7's Fast Healthcare Interoperability Resource (FHIR).

There is no reference to emergency EHI access procedures ('break the glass') when individuals need to obtain patient information in emergent situations.

We recommend that ONC consider exporting these detailed terms and conditions into a separate document that can be used by QHINs and HINs as reference, and allow for non-prescriptive, external technical architectures to be referenced and used independent of the agreement itself.

Comments on Definitions

- QHIN: One of the requirements of a QHIN is to be "participant neutral." The document noted that a regional or state HIE would not qualify. The definition provided does not clearly state why. A clear, documented definition is required.
- Connectivity Broker: While this is defined as a **service** provided by a QHIN, it sometimes is confused with a separate **entity** connected to the QHIN. It will be helpful to clarify this point and emphasize that the term 'broker' does not refer to a separate entity.
- Electronic Health Information: It is not clear if the definition includes only **identifiable** health information (whether electronic protected health information or electronic identifiable health information not considered 'protected' because it is not covered by HIPAA) or whether the term also includes non-identifiable health information.

Comments on Requirements of Qualified HINs

- We are concerned that QHINs will be expected to update data formats and APIs within 12 months of when new data classes are officially added to the USCDI. Similarly, the expectation that QHINs conform to an API implementation guide within 12 months of formal adoption by HL7 is an aggressive timeline. A more reasonable timeframe would be 24 months.
- The document references compliance with updates to standards, implementation specifications, or certification criteria to happen 12 months after they have been formally adopted by HHS. However, the document is silent regarding the adoption of new standards for existing or new transactions.

Comments on Requirements on Standardization

- The requirements specified for the connectivity broker service (or entity) seems to be extremely prescriptive with predefined approaches for handling query/responses, patient matching and other elements of the orchestration envisioned.
- Many of the detailed, prescriptive elements of the proposed approach have yet to be tested in a real, operational environment. It seems premature to establish this level of detailed conditions, terms, and requirements in a formalized common agreement.
- There is also no mention of specific limitations in the use and disclosure of identifiable health information such as minimum necessary. While HIPAA permits, in certain circumstances, a covered entity to rely on the judgement of the entity requesting the data when the requesting entity is another covered entity or a public health authority, such limitation still applies to any non-covered entity requesting to access health

information. Such non-covered entities (notwithstanding the individual consumer/patient) will be among those participating in a HIN as end users.

Comments on Requirements on Transparency

- The fee schedule approach seems to be prescriptive and controlled by ONC. It is not clear whether ONC has the jurisdictional authority to control the fees charged for such services.
- We agree with the expectation that QHINs make available standard agreements, participating agreements, USCDI data classes, and information related to patient safety, quality improvement, and public health.

Comments on Requirements on Cooperation and Non-Discrimination

- While we agree with non-discrimination provisions, there is also a need to define situations when participants will need to be excluded from a HIN/QHIN because of non-conformance, without such actions being considered discriminatory actions.
- With respect to the fees section, it seems unreasonable, complex and too prescriptive to define the level or amount that a QHIN may charge for services (such as "... a responding QHIN may charge an initiating QHIN an amount equal to the responding QHIN's attributable costs for responding to Queries/Pulls by the initiating QHIN only if they were incurred for the Permitted Purposes of TPO [Treatment, Payment, and Health Care Operations] ...")
- There also seems to be a restrictive provision that will not permit QHINs to enter into any agreement other than the Common Agreement with another QHIN.

Comments on Requirements on Privacy, Security and Patient Safety

1. Privacy:

- Generally, we agree and support all provisions of this section.
- With respect to consent, there would be at least two different aspects to consider: consent to use and disclose health information and consent to permit the exchange of patient identifiable information through a HIN/QHIN. The document does not make such distinction.
- It seems also burdensome, complex, and, in some ways, unrealistic to expect that a QHIN will be able to obtain and maintain all patient consents for all purposes of all patients that are served by end users (providers, health plans, others) that participate in a HIN and then make them available to other QHINs (so that they can, presumably, make them available to their participating HINs and end users).
- Revocation of consent: here again the focus is on consent to use and disclose, and the section is silent on consent to allow the exchange of data via the HIN/QHIN.
- There is a description of the need to have methods for individuals to submit requests for no data exchange. This seems to imply that the approach is expected to follow an opt-out policy for patients/individuals to withdraw from having their data be transferred via the HIN/QHIN network-of-networks. This may be inconsistent with existing state or private HINs.

2. Security

- The document identifies, documents and prescribes in significant detail the security expectations of QHINs. Instead of having to prescribe all these elements, the document can define the expectation that QHINs will need to meet the more than 50 security standards and implementation specifications established by the HIPAA Security Rule. In many ways, the level of prescriptive details introduces potential inconsistencies with already mandated HIPAA security requirements, duplications and unnecessary complexities.
- The document prescribes specific elements, procedures and standards for multiple areas, including data integrity, access control/authorization, identity proofing, authentication, credential management, transport security, certification policies, and policy binding, auditable events, cryptography, IP whitelisting, and incident response. Such level of prescriptive terms and conditions seems complex, costly and untested. This approach may result in both unintended consequences and high implementation costs, which will in turn increase the cost of participation and deter participation and data flow.
- In some sections, the expectations on QHINs include mandating the use of standards that are not yet adopted by HHS (a requirement defined elsewhere in the document). These provisions also identify and prescribe standards that point to specific technology solutions, architectures, infrastructures, or models. For example, the document references SOAP-based transactions when implementing access control mechanisms.

Comments on Requirements on Access

- See comments above regarding individual request for no data exchange (opt-out).

Comments on Requirements on Data-Driven Choice

- With respect to population level data, it is important to clarify whether the system is intended to support both data queries for PHI of a group of individuals that meet specified search criteria and data queries for non-identifiable PHI of as many individuals to satisfy a search.

Comments on Requirements on Participant Obligations

- The document selectively identifies a series of terms, conditions and requirements that participants would be expected to comply with. As stated in the above overall comments, there are many requirements that seem to be too prescriptive, complex and expensive to implement. Many also seem to be duplicative with HIPAA security requirements with which business associates must comply.
- As with the QHIN recommendation, here it will be much simpler, equally effective, flexible and scalable to require that participants adhere to all HIPAA security requirements.

Comments on Requirements on End User Obligations

- As with the previous section, the requirements being imposed on end users seem to be redundant at best and potentially conflicting at worst (with existing HIPAA requirements, breach notification requirements, and other federal and state laws).

Part 3: Comments on the U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process

Overall Comments

While the document mentions the Common Clinical Data Set (CCDS), defined by ONC in 2015 for Meaningful Use purposes, it is not clear how that core data set and the proposed USCDI relate to each other. It is explained in the document that the USCDI builds on the CCDS and adds two additional data classes (clinical notes and provenance). However, it is not clear whether the USCDI will replace CCDS, or whether the two will continue to exist only for different purposes.

While we understand the benefits of defining a core data set for interoperability, we are concerned that the USCDI document, together with the TEFCAs, could be seen as limiting the data that are exchanged through the QHIN/HIN network-of-networks to only those data classes.

Public health data go beyond these data classes, as do many other health-related data exchanges. We recommend this be considered a minimum core data set, rather than the core data set. We also recommend that all other data (including the so-called candidate status data classes and the emerging data classes) be allowed to be exchanged voluntarily between entities and that nothing in the TEFCAs restrict the ability of lawful health data exchange.