HL7®
International

June 13, 2019

Don Rucker, MD
National Coordinator
Office of the National Coordinator for Health Information Technology (ONC)
Department of Health and Human Services (HHS)
Mary E. Switzer Building
300 C Street SW
Washington, DC 20201

Attention: Trusted Exchange Framework and Common Framework (TEFCA) Draft 2

Submitted electronically to: https: https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement

Dear Dr. Rucker:

Health Level Seven (HL7®) International welcomes the opportunity to submit comments on the Trusted Exchange Framework and Common Framework (TEFCA) Draft 2.

HL7 is a not-for-profit, ANSI-accredited standards developing organization (SDO) dedicated to providing a comprehensive framework and related interoperability standards, including the rapidly evolving Fast Healthcare Interoperability Resources (HL7® FHIR®), the Consolidated Clinical Document Architecture (C-CDA®), and the widely used V2 messaging standards. We have more than 1,600 members from over 50 countries. HL7 greatly values its on-going collaboration with ONC and other federal government agencies to ensure that the products of our organization positively impact the lives of many Americans, providing the underpinnings for connected, patient-centered healthcare and an information highway for precision medicine.

HL7 appreciates and supports the role of the TEFCA Draft 2 in furthering the ONC goals of:

- Providing a single "on-ramp" to nationwide connectivity;
- Ensuring electronic information securely follows you when and where it is needed; and
- Supporting nationwide scalability for network connectivity.

As we emphasized in HL7's February 2018 comments on Draft 1 of the TEF these ONC goals are "solid principles for all stakeholders: a single minimum set of rules from which to operate, pursuing more efficient approaches to sharing that build on existing initiatives and focusing on private sector consensus standards and a private sector Recognized Coordinating Entity (RCE)."

We are pleased that ONC proposes the HL7® Fast Healthcare Interoperability Resources (FHIR®) RESTful API in the Qualified Health Information Network (QHIN) Technical Framework (QTF) Draft 1 as an Alternative/Emerging Standard or Profile in several critical areas. HL7 FHIR® is well positioned to support the collaborative use of FHIR-based standards as the QTF evolves and to help ensure that a patient's electronic health information (EHI) is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient, healthcare providers and other individuals.

HL7 also appreciates that its feedback and that of other key stakeholders expressed in February 2018 comments on the TEF is reflected in the TEFCA Draft 2 by:

- Adding a separate QHIN Technical Framework (QTF) distinct from the legal terms of the Common Agreement;
- Extending the compliance timeline for QHINs to update agreements and technical requirements from 12 to 18 months;
- Refining the exchange modalities, as well as QHIN pre-requisites, to better reflect today's healthcare practice and market realities; and
- Continuing to provide strong support for the concept of an RCE and its intended scope of responsibilities.

We provide detailed comments in the Appendix to this letter on all three portions of TEFCA Draft 2 including the:

- Trusted Exchange Framework (TEF) Draft 2;
- Minimum Required Terms and Conditions (MRTCs) Draft 2; and
- QHIN Technical Framework (QTF) Draft 1.

Our comments outline overarching observations on standards and resources, as well as constructs, implementation, timelines and other issues. Detailed and technical recommendations, as well as answers to specific ONC requests to comments are in our comment Appendix. High-level themes of HL7's comments are below.

The QTF and HL7 Standards - HL7 is pleased that ONC identifies the HL7® Fast Healthcare Interoperability Resources (FHIR®) RESTful API in the Qualified Health Information Network (QHIN) Technical Framework (QTF) Draft 1 as an Alternative/Emerging Standard or Profile in several critical areas. HL7 FHIR® is well positioned to support the collaborative use of FHIR-based standards as the QTF evolves and to help ensure that a patient's electronic health information (EHI) is accessible to a patient and the patient's designees, in a manner that facilitates communication with the patient, healthcare providers and other individuals. HL7 strongly emphasizes the importance and need for its implementation guides regarding the potential use of the HL7 FHIR RESTful API referenced in the QTF and in reference to the ONC QTF Request for Comment #6 that asks for insights on other appropriate standards to consider for implementation to enable more discrete data queries, such as emerging IHE profiles leveraging RESTful APIs and/or use of HL7 FHIR. Orderly, informed and fully successfully implementation of an HL7 standard or API is facilitated by implementation guides. If further HL7 implementation guide development is required in relation to the QTF, HL7 and its expert Work Groups stand ready to do so, given appropriate resources, and to appropriately assist both ONC and the RCE.

HL7 and the Recognized Coordinating Entity (RCE) - There is much critical work to be done by the RCE. HL7, as a key developer of standards that empower global health data interoperability, stands ready as an active, innovative partner to provide appropriate expertise and support to the RCE and ONC in their relevant tasks. Standards development organizations (SDOs) are a critical private sector voice. HL7 emphasizes that ONC should encourage the RCE to engage, on an on-going and systematic basis, with applicable SDOs including HL7, on issues related to TEFCA Draft 2.

TEFCA, Exchanges and QHIN Requirements/Structure - HL7 cautions ONC to be very mindful the Congressional intent that the TEFCA avoid disruption and duplication of "existing exchanges between participants of health information networks." HL7 agrees with ONC that the TEFCA should not dictate internal requirements or structures of QHINs or their components.

Exchange Modalities - HL7 supports the initial exchange modality set specified by ONC. We are concerned that data segmentation use across these exchange modalities is inadequately supported by Consent2Share, which is proposed for use by ONC. HL7 specifically supports the inclusion of QHIN Message Delivery (push modality) in the TEFCA. This modality is a key part of interoperability, and especially important for the public health community. It will likely be important to the TEFCA's success.

TEFCA and Public Health - HL7 appreciates the explicit inclusion of the public health community as a key stakeholder in and contributor to TEFCA, given its centrality to ensuring better patient and population health.

TEF Draft 2 Principle 1: **Standardization** - HL7 has a deep interest and experience in standardization as a global**,** ANSI-accredited SDO providing a comprehensive framework and related interoperability standards. We urge that any standardization efforts conducted under Principle 1 are carried out in an open and transparent manner, consistent with ANSI essential requirements, with broad stakeholder engagement and governance that appropriately balances relevant interests. HL7 agrees with the ONC approach for HINs to use standards-based technology to exchange EHI with other HINs, that such technology should be implemented in accordance with authoritative best practices published by an applicable SDO and in instances where none of the above references include applicable standards, HINs should consider voluntary consensus or industry standards that are readily available to all stakeholders.

TEF Draft 2 Principle 2: Transparency - While supporting the effort to make supported Exchange Purposes transparent, HL7 seeks clarification on how the discussion accompanying this principle aligns with prohibition against information blocking as well as with MRTC requirements for QHINs to support all Exchange Purposes and for Participants, and Participant Members to respond to queries for all MRTC-designated Exchange Purposes with EHI.

TEF Draft 2 Principle 4: Privacy, Security, and Safety - HL7 has consistently supported these principles and has developed interoperable standards across HL7 product family to technically support them. Our organization stands ready to assist with further development as deemed necessary.

TEF Draft 2 Principle 5: Access - HL7 believes that the underlying intent of Principle 5 is positive but that the framework and API provisions that it lays out require significant revision and a shift away from treating HINs as having the same responsibilities as Covered Entities to implement the HIPAA individual right of access, including through APIs. ONC should not seek to layer on top of a model of HIN exchange, the complementary model of API access for individuals and their designated apps.

TEF Draft 2 Principle 6: Population-Level Data - We agree with ONC's assessment of standards maturity and emphasize that HL7 is deeply involved in progressing the population-based exchanges envisioned by the *21st Century Cures Act* and related to this principle, while preserving privacy and safeguarding the security of data subject information being exchanged. For example, in addition to supporting this use case in HL7® FHIR® Release 4, we are developing Privacy Preserving Filtering specifications based on HL7 security labeling standards.

Minimum Required Terms and Conditions (MRTC) Development and Update - HL7 strongly emphasizes that ONC should employ a fully collaborative approach in working with a wide range of healthcare and industry stakeholders including SDOs, to modify and update the MRTCs Draft 2. This hands-on, interactive method is the best avenue to ensuring MRTCs that reflect market realities and facilitate an optimal, orderly and smooth glide path to healthcare change. ONC's work and consultation with RCE on the MRTCs is also critical. HL7 believes that the RCE should have a key role in finalizing the MRTCs.

Additional Required Terms and Conditions (ARTCs) - HL7 supports designating the RCE with responsibilities to develop the Additional Required Terms and Conditions (ARTCs). We believe that the RCE should also have an important role in finalizing the MRTCs.

1. Definitions (Exchange Purposes) - HL7 is concerned that the proposed narrowing of Exchange Purposes could preclude use of the TEFCA for valuable exchange taking place today in current models. In particular, HL7 requests a clarification and expansion in the MRTC Exchange Purposes by ONC to ensure that care coordination is included.

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

2.2.11 No EHI Outside the United States - HL7 urges ONC not to apply overly restrictive limitations on the security and privacy of EHI sent, stored, maintained, or used by QHIN Participants and Participant Members in a global context. The role of and appropriate EHI authorization by caregivers with respect to cross-border data flows, especially when health systems span international borders (e.g., U.S. and Canada) should also be carefully considered and acknowledged in this context. As healthcare becomes more globally provided due to international employment situations, healthcare tourism and other scenarios, HL7 encourages ONC to undertake a more forward-thinking approach to TEFCA policies in this area. HL7 suggests that ONC develop guidance for responding to "Break the Glass" scenarios where cross-border information flows are imperative for patient health and safety.

2.2.2 Permitted and Future Uses of EHI - HL7 urges ONC to provide clarity regarding when non-HIPAA covered entities or business associates are subject to all HIPAA privacy and security provisions. The applicability of these provisions is not fully evident in the MRTCs. HL7 commends ONC for recognizing the negative effects of not requiring non-HPAA entities adherence to HIPAA Privacy and Security rules would have on EHI exchange at all levels, including but not limited to participation of Individual Users.

2.2.3 Individual Exercise of Meaningful Choice - Meaningful Choice is a complex new concept that will require considerable effort from both the public and private sectors to implement effectively. Indeed, the infrastructure to fully launch and sustain Meaningful Choice does not now exist. HL7 urges ONC to carefully weigh these considerations and formulate appropriate and reasonable Meaningful Choice implementation timelines. HL7 believes ONC must clarify the data use status and any additional authorization procedures required for relevant EHI collected or exchanged in the context of an electronic health record prior to the implementation of Meaningful Choice. Given Meaningful Choice issues relate to important issues of privacy and security, we suggest that ONC allow less global Meaningful Choice than proposed initially, and then refine these working with the community and the RCE to provide support for more granular Individual choice about recipients, information content, and information confidentiality, especially as increasingly robust data segmentation is more widely adopted.

2.2.4 Processing of Individual Access Services Request - HL7 supports the MRTC requirement for non-HIPAA entities participating in the Common Agreement to support the Individual Access Services Exchange Purpose. HL7 recommends development of a FHIR standard for Individual Access Service Directive, which would ease the burden of implementation, create a consistent user-friendly experience for Individual Users, and promote innovative app development.

3. Data Quality and Minimum Necessary: 3.3 Minimum Necessary Requirements - HL7 is concerned that without more guidance on how the Minimum Necessary requirement can be determined in a consistent manner, Individuals may not trust that their information is adequately protected against unnecessary disclosures. We recommend that ONC and OCR work with HL7 to develop best practice standards for computably determining the appropriate type of information to disclose for compliance with Minimum Necessary Requirement for applicable Exchange Purposes.

4. Transparency: 4.1.1 Access to Participant-QHIN Agreements including Fees - HL7 is concerned about removal of language present in TEFCA Draft 1 regarding fees applied to queries for public health purposes. It is not clear what the implication is if public health related queries are not exempted from fees.

6. Privacy Requirements:

6.1.1 Breach Notification Requirements and Security Incidents - HL7 supports uniform Breach Notification Requirements for HIPAA and non-HIPAA QHINs, Participants, and Participant Members, which do not supplant any HIPAA or FTC breach reporting requirements or responsibilities.

6.2 Minimum EHI Security Requirements - HL7 recommends that ONC assess the viability and burden of requiring private sector organizations (QHINS) to conduct security assessments related to NIST Special Publication 800-171. ONC should also closely examine the applicability of the CUI requirements to the private sector.

6.2.3 Authorization - HL7 strongly supports the need for written authorization procedures but recommends that ONC work with appropriate SDOs -- including HL7 -- to further develop security labels for attribute based access control in accordance with NIST SP 800-162, Guide to ABAC Definition and Considerations—https://csrc.nist.gov/publications/detail/sp/800-162/final.

6.2.4 Identity Proofing - HL7 supports adoption of identity proofing at a minimum of IAL2.

6.2.5 User Authentication - HL7 supports TEFCA entity authentication at a minimum of AAL2, and support for non-Individual Users for at least FAL2.

9. Individual Rights and Obligations: 9.5.3 Exceptions: Right to Receive Summary of Disclosure of EHI - HL7 seeks clarification as to whether disclosures made without authorization to Health Oversight Agencies are subject to an Individual's Right to Receive Summary of Disclosures of EHI. This clarification will assist HL7 efforts to develop Accounting of Disclosure standards such as a profile on FHIR Provenance Resource for this use case.

Security Labeling - HL7 recommends that the issue of security labeling should be addressed at a later point in time through revision to the initial ARTCs. HL7 supports initial inclusion of security labels at the header level as an initial requirement to support nationwide Sharing with Protections, although we recognize that this approach to labeling can impede the freer flow of information that can be achieved by applying labels at the portion level.

The QTF and the Common Agreement - HL7 strongly supports ONC's proposal that, in a change from TEFCA Draft 1, the Qualified Health Information Network (QHIN) Technical Framework (QTF) would be incorporated by reference in the Common Agreement (CA) and finalized by and maintained by the RCE using an open, transparent and participatory governance process.

The QTF and Exchange Modalities - ONC focuses in the QTF on QHIN-to-QHIN exchange of information and specification of standards in the QTF only in relation to QHIN-to-QHIN exchange. HL7 agrees with TEFCA only specifying technical exchange standards at the level of QHIN-to-QHIN exchange and not seeking to dictate models of sub-QHN exchange beyond the applicable MRTCs. HL7 agrees with ONC that, "QHINs, Participants, and Participant Members are in no way limited from voluntarily offering additional exchange modalities and services or from entering into point-to-point or one-off agreements between organizations that are different from the Common Agreement's MRTCs, provided that such agreements do not conflict with the policies of the Common Agreement."

User Authentication – Regarding Standards for Authorization & Exchange Purpose, HL7 recommends that ONC and IHE, along with the RCE, evaluate a move, initially or in revisions to the QTF, to XSPA 2.0, which references HL7 Purposes of Use (POU) rather than a hard-coded list of non-standard POU codes. HL7 proposes that any future reference to XSPA SAML profile point at the latest version, i.e. Version 2.0 of XSPA SAML profile. This version provides a soft-update to some of the existing attributes by considering them deprecated, but still valid in order to give vendors the flexibility of a gradual upgrade. See http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html. The HL7 Security Work Group is developing a change request for this update to IHE.

Query: RE XCPD and XCA for QHIN Query Obligations - HL7 agrees with the initial focus on mature IHE profiles (implemented through appropriate implementation guides and specifications as determined by the RCE). We also support identification of the Alternative/Emerging Standard/Profiles, especially those based in HL7® FHIR® as a migration path from the Specified Standard/Profiles listed in order to move toward a mixed ecosystem of legacy and emerging standards and technologies with clear signals about the exchange ecosystem envisioned for TEFCA.

HL7 Work Groups submitted feedback on relevant questions posed by ONC. In addition to our Policy Advisory Committee, HL7 Work Groups contributing to these comments include:

- Security
- Public Health

Should you have any questions about our attached comments, please contact Charles Jaffe, MD, PhD, Chief Executive Officer of Health Level Seven International at cjaffe@HL7.org or 734-677-7777. We look forward to continuing this discussion and offer our assistance to HHS and ONC.

Sincerely,

Calvin E. Beebe

Charles Jaffe, MD, PhD
Chief Executive Officer
Health Level Seven International

Calvin Beebe
Board of Directors, Chair
Health Level Seven International

Appendix: HL7 Detailed Responses to TEFCA Draft 2

Below are detailed responses to the Trusted Exchange Framework and Common Framework (TEFCA) Draft 2.

Overarching Issues

HL7 and the Recognized Coordinating Entity (RCE)

In order to meet the goals of the *21st Century Cures Act*, build on existing work done by the industry, and scale interoperability nationwide, ONC will select a Recognized Coordinating Entity (RCE) to develop, update, implement and monitor compliance with the Common Agreement and the QTF on behalf of ONC, among other functions.

Comments:

- There is much critical work to be done by the RCE. HL7, as a key provider of standards that empower global health data interoperability, stands ready as an active, innovative partner to provide appropriate expertise and support to the RCE and ONC in their relevant tasks. Standards development organizations (SDOs) are a critical private sector voice. HL7 emphasizes that ONC should encourage the RCE to engage, on an on-going and systematic basis, with applicable SDOs including HL7, on issues related to TEFCA Draft 2.
- HL7 agrees with ONC that an experienced private sector RCE should implement and monitor compliance with the Common Agreement**.**

TEFCA, Exchanges and QHIN Requirements/Structure

Comments:

- HL7 concurs with ONC that the TEFCA should not dictate internal requirements or structures of QHINs or their components.
- HL7 cautions ONC to be very mindful the Congressional intent that the TEFCA avoid disruption and duplication of "existing exchanges between participants of health information networks."

Exchange Modalities

ONC received a number of requests from commenters to include a "push-based" exchange modality in the TEF and the Common Agreement. Commenters noted that push transactions play a vital role in supporting transitions of care and public health use cases and would be necessary to fully support required Public Health reporting. Therefore, ONC has included QHIN Message Delivery, which supports instances where a QHIN sends EHI to one or more QHINs for delivery. We request comment on the inclusion of QHIN Message Delivery and its definition.

Comments:

- HL7 supports the initial exchange modality set. We are concerned that data segmentation use across these exchange modalities are inadequately supported by Consent2Share, which is proposed for use by ONC. We elaborate on this rationale in our security label comments contained in this Appendix and in previous comments to ONC, in particular on the proposed rule *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program.*
- HL7 specifically supports the inclusion of QHIN Message Delivery (push modality) in the TEFCA. This modality is a key part of interoperability, and especially important for the public health community, and will likely be important to the TEFCA's success.

- HL7 recommends that the HL7 FHIR Standards identified for "push messaging" in the future include "FHIR Messaging" (bundle and message header), if messages are to be routed though the QHIN.
- We emphasize to ONC that HL7 has developed security labeling syntax for its main product families, HL7 Version 2, CDA, and FHIR, using the same security label vocabulary established by the HL7 Privacy and Security Healthcare Classification System (HCS). We are well underway in establishing a model transform service specification to enable the persistence of security labels on content, whenever it is transformed among these syntaxes.

TEFCA and Public Health

Comments:

- HL7 greatly appreciates the explicit inclusion of the public health community as a key stakeholder in and contributor to TEFCA, given its centrality to ensuring better patient and population-based health.

Trusted Exchange Framework (TEF) Draft 2 (Appendix 1)

The Trusted Exchange Framework (TEF) Draft 2 describes a common set of principles that facilitate trust between HINs. These principles serve as "rules of the road" for nationwide electronic health information exchange. The six principles are:

- Principle 1 – Standardization: Adhere to industry and federally recognized standards, policies, best practices, and procedures.
- Principle 2 – Transparency: Conduct all exchange and operations openly and transparently.
- 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.
- Principle 4 – Privacy, Security, and Patient Safety: Exchange EHI securely and in a manner that promotes patient safety, ensures data integrity, and adheres to privacy policies.
- Principle 5 – Access: Ensure that individuals and their authorized caregivers have seamless access to their EHI.
- 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.

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

ONC states HINs should adhere to federally adopted standards for EHI and interoperability. 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. In instances where none of the above references include applicable standards, HINs should then consider voluntary consensus or industry standards that are readily available to all stakeholders, thereby supporting robust and widespread adoption. HINs should use standards-based technology to exchange EHI with other HINs. To minimize variation in how standards are implemented, such technology should be implemented in accordance with authoritative best practices published by an applicable standards development organization (SDO).

Comments:

- HL7 possesses both deep interest and experience in standardization as a global**,** ANSI-accredited SDO providing a comprehensive framework and related interoperability standards. We urge that any standardization efforts conducted under Principle 1 are carried out in an open and transparent manner, consistent with ANSI essential requirements, with broad stakeholder engagement and governance that appropriately balances relevant interests.
- HL7 agrees with the ONC approach for HINs to use standards-based technology to exchange EHI with other HINs, that such technology should be implemented in accordance with authoritative best practices published by an applicable SDO and in instances where none of the above references include applicable standards, HINs should consider voluntary consensus or industry standards that are readily available to all stakeholders. HL7 strongly and consistently advocates for use of accredited standards that meet all ANSI essential requirements within the voluntary standards consensus process. The provisions under Principle 1 align with these principles.
- Relevant adopted standards should comprise exclusively accredited American National Standards, or consortia consensus standards that meet all provisions of the WTO TBT Agreement or the ANSI Essential Requirements (per NTTAA and OMB circular 119). Unaccredited implementation guidance for these standards, such as data specifications for government quality measures, should be promulgated only through sub-regulatory publications that can be updated when needed.

Principle 2 – Transparency: Conduct all exchange and operations openly and transparently.

A. Make terms, conditions, and contractual agreement that govern the exchange of EHI easily and publicly available.

ONC states that, while some HINs currently support all the uses and disclosures specifically addressed in the HIPAA Privacy Rule, others may only support use and disclosure of electronic protected health information (ePHI) for treatment purposes. When HINs have varying, allowable uses and disclosures in their own data use agreements, the full exchange of EHI between those HINs is limited. Therefore, HINs should specify the minimum set of uses and disclosures they support. These should be specified in the HINs legal agreement with their participants, made open and transparent consistent with Principle 2.A, and clearly communicated when EHI is requested or sent between participants and HINs.

Comments:

- While supporting the effort to make supported Exchange Purposes transparent, HL7 seeks clarification on how the discussion accompanying this principle aligns with prohibition against information blocking as well as with MRTC requirements for QHINs to support all Exchange Purposes and for Participants, and Participant Members to respond to queries for all MRTC-designated Exchange Purposes with EHI that they have available, subject to certain conditions (e.g., compliance with law and "minimum necessary').

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.

Comments:

- HL7 has consistently supported these principles and has developed interoperable standards across HL7 product family to technically support them. Our organization stands ready to assist with further development as deemed necessary.

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

A. Do not impede or put in place any unnecessary barriers to the ability of individuals to access and direct their EHI to designated third parties, and to learn how information about them has been access or disclosed.

ONC states that HINs that maintain EHI should (1) enable individuals to easily and conveniently access their EHI; (2) enable individuals to direct their EHI to any desired recipient they designate; and (3) ensure that individuals have a way to learn how their information is shared and used. Much like the HIPAA law provisions on individuals' access to their health information are important, for purposes of this Principle, ONC states HINs should not limit third party applications from accessing individuals' EHI via an API when the application complies with the applicable data sharing agreement requirements and the individual has directed the entity to disclose a copy of ePHI to the application.

Comments:

- HL7 believes that the underlying intent of Principle 5 is positive but that the framework and API provisions that it lays out require significant revision and a shift away from treating HINs as having the same responsibilities as Covered Entities to implement the HIPAA individual right of access, including through APIs. ONC should not seek to layer on top of a model of HIN exchange, the complementary model of API access for individuals and their designated apps.
- HL7 has consistently supported the core concepts under Principle 5 and has developed interoperable standards across HL7 product family to technically support them. We stand ready to assist with further development as deemed necessary.

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.

ONC notes that standards to support this use case are not yet mature enough for widespread implementation. As updated and new standards become available, HINs should provide the ability for their participants to both pull and push population level records. This decreases the amount of time a clinician's resources are devoted to such activity and makes more time available for providing efficient and effective care.

Comments:

- We agree with ONC's assessment of standards maturity but emphasize that HL7 is deeply involved in progressing the population-based exchanges envisioned by the *21st Century Cures Act* and related to this principle, while preserving privacy and safeguarding the security of data subject information being exchanged. For example, in addition to supporting this use case in HL7® FHIR® Release 4, we are developing Privacy Preserving Filtering specifications based on HL7 security labeling standards such as the Privacy Aware Bulk Data Access demonstration at the 2019 Connectathon— https://confluence.hl7.org/download/attachments/51216537/Privacy-Aware-Bulk-Data-Transfer-20190426.pptx?version=1&modificationDate=1556427272617&api=v2.

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

MRTC Development and Update

Congress charged ONC in the *21st Century Cures Act* with ensuring full network-to-network exchange of EHI through a Trusted Exchange Framework and Common Agreement (TEFCA). The TEFCA Draft 2 document outlines an updated version of Minimum Required Terms and Conditions (MRTCs) to ensure that signers of the Common Agreement accede to common practices and align to the principles and objectives contained in the TEF. ONC intends to update and release a Final TEF, while working with the RCE and industry stakeholders to modify and update the MRTCs Draft 2 and the QTF Draft 1.

Comments:

- HL7 strongly emphasizes that ONC should employ a fully collaborative approach in working with a wide range of healthcare and industry stakeholders including SDOs, to modify and update the MRTCs Draft 2. This hands-on, interactive method is the best avenue to ensuring MRTCs that reflect market realities and facilitate an optimal, orderly and smooth glide path to healthcare change. ONC's work and consultation with RCE on the MRTCs is also critical. HL7 believes that the RCE should have a key role in finalizing the MRTCs.

Additional Required Terms and Conditions (ARTCs)

In addition to the MRTCs, the Common Agreement would include Additional Required Terms and Conditions (ARTCs) that are necessary for an effective data sharing agreement. These may include provisions that govern interactions between the RCE and the QHINs. The ARTCs are developed by the RCE and approved by ONC. The Recognized Coordinating Entity (RCE) will combine the MRTCs with the ARTCs into a full data sharing agreement -- known as the Common Agreement -- with which QHINs may voluntarily agree to be bound.

Comments:

- HL7 supports designating the RCE with responsibilities to develop the Additional Required Terms and Conditions (ARTCs). We believe that the RCE should also have an important role in finalizing the MRTCs.
- As with the MRTCs, HL7 emphasizes that ONC and the RCE should employ a fully collaborative approach in working with a wide range of healthcare and industry stakeholders including SDOs, to develop the ARTCs. ONC's work and consultation with RCE on the ARTCs is vital. This approach is the optimal route to ensuring the ARTCs represent, reflect and balance fairly the interests of key healthcare constituencies.

1. Definitions (Exchange Purposes)

All entities participating in the QHIN Exchange Network must sign an appropriate Framework Agreement (i.e., Common Agreement, Participant-QHIN Agreement, or Participant Member Agreement) and are thereby authorized to request use of core functions of the QHIN Exchange Network. The MRTCs require that all requests to send and receive EHI fall under a defined set of Exchange Purposes, with a proposed narrowing of the HIPAA Payment and Healthcare Operations Exchange Purposes: use or disclosure for treatment, utilization review, quality assessment and improvement, business planning and development, public health, individual access services and benefits determination, each to the extent permitted under applicable law. EHI may be requested, exchanged, retained, aggregated, used or d for an Exchange Purpose under Sections 2.2,1, 7.1, 8.1 below only for an Exchange Purpose of a Covered Entity or other healthcare provider that is acting in accordance with applicable law; provided, however, that this requirement shall not apply to individual access services or benefits determination. The Common Agreement will initially require exchange for only a subset of activities in Payment (Utilization Review) and Health Care Operations (Quality Assessment and Improvement, and Business Planning and Development) as defined in the HIPAA Privacy Rule.

Comments:

- We are concerned that the proposed narrowing of Exchange Purposes could preclude the use of the TEFCA for valuable exchange that is taking place today in current models. In particular, HL7 requests a clarification and expansion in the MRTC Exchange Purposes by ONC to ensure that care coordination is included.

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

2.2.11 No EHI Outside the United States

ONC states in the TEFCA Draft 2 that with respect to activities that are subject to specific terms and conditions and the Common Agreement, no QHIN shall use or disclose any EHI outside the United States except as required by Applicable Law or as provided below.

- QHINs shall not use or disclose any EHI to any person or entity outside the United States (or allow any third party acting on its behalf to take such action) except to the extent that an Individual User requires his or her EHI to be used or disclosed outside of the United States.

- QHINs may only utilize cloud-based services that are physically located within the United States. All EHI provided to a cloud services provider shall be stored physically within the United States and shall not be transferred to or located in any other countries or jurisdictions.

ONC seeks public comment on how the Common Agreement should handle potential requirements for EHI that may be used or disclosed outside the United States. Currently, the MRTCs Draft 2 does not permit QHINs to use or disclose EHI outside the United States, except to the extent that an Individual User requests his or her EHI to be used or disclosed outside of the United States. ONC requests comment on reasonable applicability of similar limitations to preserve the security and privacy of EHI sent, stored, maintained, or used by Participants and Participant Members while also preserving the rights of each Individual with respect to that EHI.

Comments:

- HL7 possesses notable experience in cross-border patient care record exchange through initiatives such as its Trillium Bridge project and others (Trillium Bridge was a feasibility study on the exchange of Patient Summaries between the U.S. and Europe—http://bit.ly/2K4S9AW.). From this vantage point, HL7 urges ONC not to apply overly restrictive limitations on the security and privacy of EHI sent, stored, maintained, or used by QHIN Participants and Participant Members in a global context. The role of and appropriate EHI authorization by caregivers with respect to cross-border data flows, especially when health systems span international borders (e.g., U.S. and Canada) should also be carefully considered and acknowledged in this context. Although HL7 agrees with ONC that U.S. privacy and security laws do not now govern outside of the U.S., as healthcare becomes more globally provided due to international employment situations, healthcare tourism and other scenarios, HL7 encourages ONC to undertake a more forward-thinking approach to TEFCA policies in this area.
- HL7 believes at a minimum, it would be helpful to understand the extent to which federal agencies and U.S. employers have already established exchange of health information of individuals participating in health coverage provided by these entities. It would also be useful to better understand how Individual Users may request sharing of their EHI outside of the U.S. under the protections offered by their recipient's health information statutes, e.g., sharing with European Union nations (EU), which have somewhat different approaches to implementing the General Data Protection Regulation (GDPR). In anticipation of this need, the HL7 Security Work Group has over the past year been pursuing the development of a FHIR GDPR Implementation Guide—https://confluence.hl7.org/display/SEC/FHIR+-

+GDPR?src=contextnavpagetreemode with profiles for GDPR-specific Security Labels, FHIR Consent, Contract, Audit, and Provenance Resources.

- ONC should examine relevant HL7 International Affiliate activities to obtain a fuller picture about the extent to which TEFCA could evolve to be more encompassing of international health information exchange. For example, there is the HL7 Trillium Project body of work, referred to above, for implementing EU CDA and FHIR profiles that is well underway. We know of multiple international and regional implementations of HL7 which could be leveraged to enable seamless sharing of TEFCA Individual User information across national boundaries while "sharing with protections" and being respectful of the recipient's governing laws balanced with the protection that U.S. citizens expect. We would be pleased to provide further information to ONC as and when appropriate.
- Finally, HL7 suggests that ONC develop guidance for responding to "Break the Glass" scenarios where cross-border information flows are imperative for patient health and safety.

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

2.2.2 Permitted and Future Uses of EHI

The MRTCs Draft 2 includes provisions that address QHIN, Participant, and Participant Member privacy and security practices in order to ensure all connections within a QHIN's network are trusted and secure. The MRTCs Draft 2 requires that QHINs comply with the HIPAA Privacy and Security Rules as it pertains to EHI. Also, QHINs must evaluate their security program for the protection of Controlled Unclassified Information (CUI) and develop and implement an action plan to comply with the security requirements of the most recently published version of the NIST Special Publication 800-171 (Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations). Once EHI is received by a QHIN, the recipient QHIN may exchange, retain, aggregate, use, and disclose such EHI only in accordance with Applicable Law and only for specific purposes outlined in the MRTC Draft 2. The Common Agreement requires non-HIPAA entities, which elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. Federal agencies that are not subject to HIPAA may elect to be a Participant or Participant Member. In these instances, such agencies would not be required to comply with the HIPAA Rules referenced in the Common Agreement. However, they must comply with all privacy and security requirements imposed by applicable federal law.

Comments:

- HL7 urges ONC to provide clarity regarding when non-HIPAA covered entities or business associates are subject to all HIPAA privacy and security protections. This is not fully evident in the MRTCs.
- HL7 commends ONC for recognizing the negative effects of not requiring non-HPAA entities adherence to HIPAA Privacy and Security rules would have on EHI exchange at all levels, including but not limited to participation of Individual Users.
- ONC states that a QHIN may "exchange, retain, aggregate, Use, and Disclose such EHI only in accordance with Applicable Law and only for: (i) one or more of the Exchange Purposes". In doing so, ONC seems to expect QHINs to determine whether the Exchange Purposes are permissible under HIPAA. To ease implementer burden and engender the trust of Individuals that their information is being shared in accordance with Applicable Law, HL7 recommends that ONC collaborate with OCR on guidance about how QHINs should accomplish this determination computably using a standards-based approach. in particular with respect to HIPAA Payment and Operations Exchange Purposes. For example, some HIEs determine whether a payer or provider has or has had a relationship with an Individual as required under HIPAA to exchange PHI for Payment and Operations Exchange Purposes based on whether a either has conducted a HIPAA eligibility or claims transaction related to that Individual, but this approach is non-standard and requires that the HIE have access to all provider/payer HIPAA X12 or NCPDP transactions.

- The HL7® Da Vinci Health Record Exchange Framework (HRex)—https://confluence.hl7.org/pages/viewpage.action?pageId=40741996&src=contextnavpagetreemode may provide a simpler standards-based approach to ensuring that each Individual who is the information subject being disclosed for Payment or Operations Exchange Purposes has or has had a relationship with the recipient. HL7 recommends that ONC and CMS support development of a Da Vinci FHIR Implementation Guide to establish a uniform and trusted approach to ensuring that Payment or Healthcare Operations Exchange Purposes are conducted in accordance with HIPAA and other Applicable Laws, such as 42 CFR Part 2 and Title 38 Section 7332.

2. Initial Application, Onboarding, Designation and Operation of QHINs
2.2.3 Individual Exercise of Meaningful Choice

Given the anticipated increased access in EHI exchange through the Common Agreement, it is critical that Individuals have the opportunity to understand and make informed choices about where, how, and with whom their EHI is shared. Therefore, the MRTCs require that QHINs, Participants, and Participant Members provide Individuals with the opportunity to exercise Meaningful Choice to request that their EHI not be used or disclosed via the Common Agreement, except as required by applicable law. Participants and Participant Members are responsible for communicating this Meaningful Choice to the QHIN who must then communicate the choice to all other QHINs. Participants and Participant Members are responsible for communicating this Meaningful Choice up to the QHIN who must then communicate the choice to all other QHINs. This choice must be respected on a prospective basis.

Additionally, all QHINs, Participants, and Participant Members who provide Individual Access Services must publish and make publically available a written notice describing their privacy practices regarding the access, exchange, use, and disclosure of EHI. This notice should mirror ONC's Model Privacy Notice and include information and explanation of how an Individual can exercise their Meaningful Choice and whom they may contact for more information about the entity's privacy practices.

Also relevant to these HL7 comments is section 6.14:

> 6.1.4 Other Legal Requirements. If and to the extent that Applicable Law requires that an Individual either consent to or approve the Use or Disclosure of his or her EHI to the QHIN, then each QHIN that has a Direct Relationship with the Individual shall not Use or Disclose such EHI in connection with the Common Agreement unless the QHIN has obtained the Individual's consent, approval or other documentation with respect to such Uses or Disclosures consistent with the requirements of Applicable Law. The QHIN shall maintain copies of such consent, approval or other documentation and may make it available electronically to any other QHIN upon request to the extent permitted by Applicable Law. The QHIN shall maintain written policies and procedures to allow an Individual to revoke such consent or approval on a prospective basis. Each QHIN shall specify responsibilities comparable to those described above in its Participant-QHIN Agreements and each Participant shall specify responsibilities comparable to those described above in its Participant Member Agreements.

Comments:

- Meaningful Choice is a complex new concept that will require considerable effort from both the public and private sectors to implement effectively. Indeed, the infrastructure to fully launch and sustain Meaningful Choice does not now exist. HL7 urges ONC to carefully weigh these considerations and formulate appropriate and reasonable Meaningful Choice implementation timelines.

- HL7 has concerns about the concept of Meaningful Choice specifically in relation to public health. Public health reporting mandates, opt-in/opt-out provisions, age-based requirements for reporting, age-based consent for inclusion, automated vs. manual reporting, modified or rescinded consent over time all add complexity to a nation-wide approach to interoperability. Often, public health reporting is non-optional. TEFCA implementation should not preclude TEFCA participants from supporting statutory reporting, even if Meaningful Choice has been exercised. These specific issues and others related to the intersection of law/policy and individual choice should be further addressed in the final TEFCA document.
- HL7 believes ONC must clarify the data use status and any additional authorization procedures required for relevant EHI collected or exchanged in the context of an electronic health record prior to the implementation of Meaningful Choice. These issues are not outlined in the MRTCs.
- As the Meaningful Choice concept is proposed in the MRTCs, opting out for Individuals is a global, all or nothing decision. While HL7 supports the ability of Individuals to make Meaningful Choices about whether their information is shared across the TEFCA ecosystem, this binary process does not recognize the complex realities of electronic information exchange, healthcare security and privacy or the multi-layered U.S. patient care system. HL7 urges ONC to review the intricacies involved in Meaningful Choice and develop a nuanced, stepwise Meaningful Choice framework, in working with the RCE and industry stakeholders in modifying and updating the MRTCs. Given Meaningful Choice issues relate to important issues of privacy and security, we suggest that ONC allow less global Meaningful Choice than proposed initially, and then refine these working with the community and the RCE to support for more granular Individual choice about recipients, information content, and information confidentiality, especially as more robust data segmentation is more widely adopted.
- HL7 requests additional clarification from ONC regarding:
  - We ask ONC to provide more clarification on the meaning of "respected on a prospective basis."
  - If a patient is in a HIE that never gave a choice about sharing, and is now connected through that HIE to a QHIN – can the original HIE continue to further disclose that information under the MRTCs? Or if an Individual opted in for relatively circumscribed exchange among providers in a HIE, such as limiting the content and Exchange Purposes, would that Individual's previous choice now be overridden because it was not prospective?
  - Does ONC intend that once a QHIN, Participant, or Participant Member is operating under the Common Agreement -- that Meaningful Choice begins within an initial period of notice such that if an Individual did not opt-out or opted in with restrictions on Exchange Purposes, and that the Individual's information is exchanged after inaction, that it may be used even after the Individual later chooses to opt-out or restrict Exchange Purposes? HL7 believes that ONC intends the latter scenario. In either case, clarification from ONC would be helpful.
- HL7 urges caution regarding the provisions for Individual Access Services and asks whether a public health registry that is participating in the TEFCA as a Member or Member Participant is required to respond to such a request. For example, some public health laws and rules do not allow Individuals to access their own data or they restrict how access is obtained (e.g., a state law may require the patient to come in person with photo ID for identity proofing). HL7 requests that ONC consider whether public health should be provided a specific exemption from this requirement and whether section 8.21 on page 67 of the TEFCA Draft 2 document should be revised to extend the exemption provided to federal agencies to state and local agencies.
- Without guidance, the myriad of compliance approaches related to the Individual Exercise of Meaningful Choice and Other Legal Requirements across all TEFCA entities are likely to result in inefficiencies and interactions that are not scalable. There is also potential for compliance breaches and information blocking. We urge ONC to pay careful heed to comments received on this provision.
- We also recommend that ONC engage with HL7 to develop a nationwide approach to electronic Consent Management System (eCMS) reference model that provides flexible approaches to implementing standards-based components appropriate to the exchange ecosystems deployed by Participants and their Participant Member. HL7 members have for many years, since the inception of HL7 Version 3, worked on designing and

implementing eCDMS. This experience could be leveraged to develop a reference model for use by TEFCA QHINs, Participants, Participant Members, and Individual Access Service providers to ensure that Meaningful Choice, Individual Access Service Directives, and Consents and Authorizations are available timely, seamlessly and interoperably. Not doing so risks the lack of full engagement by Individual Users in the nationwide sharing of their health information.

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

2.2.4 Processing of Individual Access Services Request

The Individual Access Services Exchange Purpose now also includes a corresponding requirement for non-HIPAA entities that elect to participate in the Common Agreement. ONC requests comment on the scope of these Exchange Purposes. Participants and Participant Members that only provide Individual Access Services are only required to respond to requests for Individual Access Services.

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

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

Comments:

- HL7 supports the MRTC corresponding requirement for non-HIPAA entities participating in the Common Agreement to support Individual Access Services Exchange Purpose because Individuals need to know what information Non-Covered Entities possess, which will increase if they choose to participate.
- HL7 supports limiting responses from Participants and Participant Members that only provide Individual Access Services to requests for Individual Access Services. Any other response obligation has the potential to be privacy invasive, unexpected by the Individual data subject and is likely dampen the willingness of Individual Users to participate, which is counter to *The 21st Cures Act* goals.
- With respect to Processing of Individual Access Services Request (i) provisions for QHIN, Participants, and Participant Members: to alleviate the cost and likely consistency of among approaches to implementing these requirements across TEFCA entities, and to improve Individual User experience exercising their right to Individual Access Services, HL7 recommends that ONC sponsor development of a standard Individual Access Service form. This form should use the FHIR Questionnaire/Questionnaire Response with automated transforms into a FHIR Individual Access Service Directive, specified by a FHIR Individual Access Service Directive Implementation Guide (IG), which could be referenced in regulatory or sub-regulatory guidance.
- A FHIR Individual Access Service IG should leverage the FHIR Consent Resource for an Individual User's unsigned right to Individual Access Services to EHI assertion and a FHIR Contract for an Individual User's signed right to Individual Access Services assertion when the Individual wants the EHI to go to a third party.
- HL7 notes that Use of FHIR Contract, which supports an inline signature, may be necessary if approving EHI disclosure to a third-party using OAuth 2.0 token is not sufficient. FHIR Consent does not include a signature, but it is possible to have it referenced by an associated FHIR Provenance Resource that documents the "signing ceremony."

- HL7 recommends developing a FHIR standard for Individual Access Service Directive, which would ease the burden of implementation, create a consistent user-friendly experience for Individual Users, and promote innovative app development.
- HL7 seeks clarification about the signature requirement at 45 CFR § 164.524(c)(3)(ii) when an Individual directs an Individual Access Service to send EHI to a third party. Does presenting an Individual with an Authorization user interface in which the Individual can select an "approval" button authorizing an Individual Access Service to send EHI to an App using OAuth 2.0 suffice as a signature for purposes of compliance?

3. Data Quality and Minimum Necessary

<u>3.3 Minimum Necessary Requirements</u>

A QHIN shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI and when the QHIN requests EHI in the context of the Common Agreement. The Minimum Necessary Requirements shall apply to a QHIN when it requests, Uses, or Discloses EHI. Any provisions in the HIPAA Rules (e.g., 45 CFR § 164.514(d)) that include conditions shall also apply to the QHIN when Using, Disclosing or requesting EHI if such provisions are applicable.

Also relevant to HL7 comments are sections 7.19 and 8.19.

> 7.19 <u>Minimum Necessary Requirements</u>. Each Participant shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI for applicable Exchange Purposes or when the Participant requests EHI in the context of the applicable Framework Agreement. The Minimum Necessary Requirements shall apply to a Participant regardless of whether it is a Covered Entity or a Business Associate when it requests, Uses, or Discloses EHI. Any provisions set forth in the HIPAA Rules (e.g., 45 CFR §164.514(d)) that include conditions shall also apply to the Participant when Using, Disclosing or requesting EHI if such provisions are applicable."
>
> 8.19 <u>Minimum Necessary Requirements</u>. Each Participant Member shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI and when the Participant Member requests EHI in the context of the applicable Framework Agreement. The Minimum Necessary Requirements shall apply to a Participant Member regardless of whether it is a Covered Entity or a Business Associate when it requests, Uses, or Discloses EHI. Any Minimum Necessary provisions set forth in the HIPAA Rules (e.g., 45 CFR §164.514(d)) that include conditions shall also apply to the Participant Member when Using, Disclosing or requesting EHI if such provisions are applicable."

Comments:

- The Minimum Necessary Requirements for a QHIN, Participant, and Participant Member are nearly identical with the exception that the phrase "regardless of whether it is a Covered Entity or a Business Associate" is not included in the Requirements for a QHIN. HL7 seeks clarification on why a QHIN's possible status as a Covered Entity or a Business Associate is not specified in the Minimum Necessary provisions.
- HL7 is concerned that without additional guidance on how the Minimum Necessary requirement can be determined in a consistent manner, Individuals may not trust that their information is adequately protected against unnecessary disclosures. We recommend that ONC and OCR work with HL7 to develop best practice standards for computably determining the appropriate type of information to disclose for compliance with Minimum Necessary Requirement for the applicable Exchange Purposes.

- HL7 observes that today there is wide variance in the manner in which Covered Entities determine the Minimum Necessary for Exchange Purposes to which it applies. That variance will likely be more evident with the increasing volume of exchanged under TEFCA. One driver of differences is that a QHIN, Participant, and Participant Member could be the Business Associate of multiple Covered Entities, which may have different criteria for determining Minimum Necessary disclosures for applicable Exchange Purposes. While it may be possible to develop agreement among trading partners as criteria for determining Minimum Necessary, as more cross QHIN and Participant exchanges occur, there could be a tendency to establish bilateral agreements about Minimum Necessary polices, which would likely not scale and might even be considered information blocking. This variance impacts the way in which Minimum Necessary disclosures are computably determined and are difficult for software vendors to implement with any consistency across customers. As a result of this variance, Individuals are more likely to find differences in the amount and kind of information being disclosed by different TEFCA entities for the same Exchange Purposes, as the sharing of their information increases.

4. Transparency

4.1.1 <u>Access to Participant-QHIN Agreements including Fees</u>

Comments:

- HL7 is concerned about removal of language present in TEFCA Draft 1 regarding fees applied to queries for public health purposes. It is not clear what the implication is if public health related queries are not exempted from fees. Does this change mean that:

  - Public health entities may need to pay for access to data held by QHINs and their participants?
  - Public Health entities may charge users for access to data held by the entity?

  Given the critical role of public health data in maintaining healthy populations, HL7 strongly advocates that the MRTCs clearly state public health entities may not be charged fees to access or receive data.

6. Privacy Requirements

6.1.1 <u>Breach Notification Requirements and Security Incidents</u>

The MRTCs Draft 2 requires that QHINs, Participants, and Participant Members comply with the Breach notification requirements pursuant to the HIPAA Breach Notification Rule at 45 CFR §164.400-414, regardless of whether they are a Covered Entity or Business Associate.

Comments:

- HL7 fully supports uniform Breach Notification Requirements for HIPAA and non-HIPAA QHINs, Participants, and Participant Members, which do not supplant any HIPAA or FTC breach reporting requirements or responsibilities.

6. Privacy Requirements

6.2 <u>Minimum EHI Security Requirements</u>

The MRTCs Draft 2 requires that QHINs comply with HIPAA Privacy and Security Rules. Also, QHINs must evaluate their security program for the protection of Controlled Unclassified Information (CUI), and develop and implement an action plan to comply with the security requirements of the most recently published version of the NIST Special Publication 800-171 (Protecting Controlled Unclassified Information in Non-federal Information

Systems and Organizations). A CUI category includes EHI. This Publication provides principle guidelines to federal government-wide requirements for CUI, and entities which handle EHI are required to demonstrate the security controls and be compliant with the NIST 800-171 requirements of the most recent publication.

To the extent the QHIN's risk analysis identifies any risks, vulnerabilities, or gaps in the QHIN's compliance with the HIPAA Privacy and Security Rules or other Applicable Law, the QHIN would be required to assess and implement appropriate security measures consistent with industry standards and best practices that it determines would be reasonable and appropriate to ensure the confidentiality, integrity and availability of the EHI that it creates, receives, maintains or transmits, and provide documentation of any such evaluation. This evaluation would not be required for Participants and Participant Members. QHINs are to evaluate their security program on at least an annual basis.

Comments:

- HL7 recommends that ONC assess both the viability and burden of requiring private sector organizations (QHINS) to conduct security assessments related to NIST Special Publication 800-171. ONC should also closely examine the applicability of the CUI requirements to the private sector.
- The HL7 Security Work Group has conducted a thorough review of CUI Authorities and has concluded that there are two CUI categories that apply to Controlled Unclassified Information disseminated by federal agencies or those acting on behalf of Federal agencies. For more information, please see Controlled Unclassified Information (CUI) Problem and Solutions—https://confluence.hl7.org/display/SEC/Controlled+Unclassified+Information+%28CUI%29+Problem+and+Solutions.
- HL7 seeks clarification from ONC about why the agency indicates that there is a "CUI Category" that includes EHI. From our analysis, both OMB Circular A-130, which governs Personally Identifiable Information, and HIPAA 42 USE 1320d(4), which governs Individually Identifiable Health Information apply to Federally disseminated information. HL7 and its Security and Community-Based Care and Privacy Work Groups would welcome further discussion of this issue.
- Additionally, HL7 notes that there is likely one default CUI security label, which would suffice for the majority of health information exchanges under TEFCA that contain Controlled Unclassified Information. Adoption of this default CUI security label would lower implementation burden and increase adoption while maximizing interoperability for systems required to meet NIST SP 800-171 security controls.
- HL7 seeks clarification from ONC about the rationale behind the following statement: "[t]his evaluation would not be required for Participants and Participant Members." Understandably, the Participants and Participant Members should not be conducting their QHIN's Risk Analysis. They should be conducting their own risk analysis, to the extent that their QHIN is a Business Associate of its Covered Entity Participants, and indirectly of those Participant's Covered Entity Participant Members, a QHIN's security posture impacts the sum of their security risk surfaces. To the extent that the QHIN risks are also risks for the underlying entities, any proposed mitigation should be vetted in that community especially where those members need to implement the same or similar mitigations.

6. Privacy Requirements
6.2.3 Authorization

ONC states, each QHIN's security policy shall include written authorization procedures to confirm that any entities requesting access to system functions or EHI possess the appropriate credentials (e.g., privileges granted and provisioned in security and privacy management).

Comments:

- HL7 strongly supports the need for written authorization procedures but recommends that ONC work with appropriate SDOs -- including HL7 -- to further develop security labels for attribute based access control in accordance with NIST SP 800-162, Guide to ABAC Definition and Considerations— https://csrc.nist.gov/publications/detail/sp/800-162/final. This approach will increase trust among TEFCA entities that security labels on information shared with protections will be enforced within recipient enterprises in the manner expected by the information discloser and by the Individual subject of the information.

6. Privacy Requirements
6.2.4 Identity Proofing

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

Comments:

- HL7 supports adoption of identity proofing at a minimum of IAL2.

6. Privacy Requirements
6.2.5 User Authentication

Each QHIN shall adhere to the user authentication functional requirements as described in the QHIN Technical Framework where applicable. Additionally, each QHIN shall require that any staff or users at the QHIN, Participants, or Individual Users who request EHI or request to send EHI shall be authenticated at a minimum of AAL2 and, if not an Individual User, also provide support for at least FAL2. Each QHIN shall also require each of its Participants to authenticate any Participant Members or Individuals Users that request EHI or request to send EHI at a minimum of AAL2 and, if not an Individual User, also provide support for at least FAL2.

Comments:

- HL7 supports TEFCA entity authentication at a minimum of AAL2, and support for non-Individual Users for at least FAL2.

9. Individual Rights and Obligations
9.5.3 Exceptions: Right to Receive Summary of Disclosure of EHI

A summary of Disclosures shall not be required for the following Disclosures: (i) for treatment, payment and health care operations (each as defined in the HIPAA Rules); (ii) to an Individual of his or her own EHI; (iii) pursuant to an

Authorization under 45 CFR 164.508 executed by the Individual; (iv) to correctional institutions or law enforcement officials; (v) for national security or intelligence purposes; and (vi) if providing the summary of Disclosures of EHI would be in violation of Applicable Law.

Comments:

- HL7 seeks clarification as to whether disclosures made without authorization to Health Oversight Agencies are subject to an Individual's Right to Receive Summary of Disclosures of EHI. This clarification will assist HL7 efforts to develop Accounting of Disclosure standards such as a profile on FHIR Provenance Resource for this use case.

Security Labeling

Currently, security labels can be placed on data to enable an entity to perform access control decisions on EHI such that only those persons appropriately authorized to access the EHI are able to do so. ONC is considering the inclusion of a new requirement regarding security labeling that states the following:

- Any EHI containing codes from one of the SAMHSA Consent2Share sensitivity value sets for mental health, HIV, or substance use in Value Set Authority Center (VSAC)—https://vsac.nlm.nih.gov/ shall be electronically labeled;
- Any EHI of patients considered to be minors shall be electronically labeled;
- The data holder responding to a request for EHI is obligated to appropriately apply electronic security labels to the EHI;
- At a minimum, such EHI shall be electronically labeled using the confidentiality code set as referenced in the HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (DS4P IG), Part 1: CDA R2 and Privacy Metadata; and
- Labeling shall occur at the highest (document or security header) level.

Comments:

- HL7 observes and recommends that the issue of security labeling should be addressed at a later point in time through revision to the initial ARTCs.
- HL7 supports the application of security labels at the header level as an initial requirement to support nationwide Sharing with Protections, although we recognize that this approach to labeling can impede the freer flow of information that can be achieved by applying labels at the portion level. Portion is the term used by 32 CFR Part 2002 for sub-parts of Controlled Unclassified Information, which may be labeled at a granular level. We use it here as a general term of art for the subparts of any content. For FHIR, the portion level could be a Resource within a Bundle or an element within a Resource. For HL7 Version 2, the portion could be a segment or a field element. For CDA, granular data segmentation is at the section or entry level.
- While HL7 agrees that using a "starter set" of sensitivity value sets for mental health, HIV, or substance use in Value Set Authority Center (VSAC) and HL7 sensitivity codes related to minors is a prudent first step, simply applying a confidentiality code of "restricted" is not sufficient for either the decision to disclose or for the recipient to comply with the applicable law, whether labeled at the document/header level or at the portion level. See HL7 Information Sensitivity— https://bcl-lab.github.io/FHIR_CG_web/v3/InformationSensitivityPolicy/vs.html code: "ADOL" (adolescent information sensitivity) which is the policy for handling information related to an adolescent. It affords heightened confidentiality per applicable organizational or jurisdictional policy.

The confidentiality protections given to sensitive information differs by applicable law. HIV sensitive information has the normative (the norm) level of confidentiality if governed by HIPAA. However, if HIV sensitive information is governed under Title 38 Section 7332, 42 CFR Part (as comorbid with substance use disorder), or under some state laws, the level of confidentiality protection is coded as "restricted", because those laws are more protective than HIPAA. The standard for the use of Confidentiality codes as established in the HL7 Privacy and Security Classification System (HCS) is discussed at the HL7 Security Work Group Confidentiality Codes—https://confluence.hl7.org/display/SEC/Confidentiality+Codes?src=contextnavpagetreemode page. For general discussion on security labeling, please see Security Labels—https://confluence.hl7.org/display/SEC/Security+Labels?src=contextnavpagetreemode.

- HL7 observes that each applicable law protecting the sensitivity conditions in the TEFCA "starter set" likely require different HL7 security control tags. To ensure sender/receiver compliance, these controls are computably enforced by different Access Control System rules. However, the referenced Consent2Share, which is not a recognized HL7 specification, only supports the security controls required by 42 CFR Part 2, and if used, would result in inappropriate information blocking of information governed under other laws.
- As we discussed in HL7's ONC *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* comments, for purposes of interoperability and Sharing with Protections across policy domains, there needs to be consensus on how to configure a security label and which privacy tags to use for any applicable security (e.g., CUI), privacy, or consent directive policy that governs EHI. HL7 stands ready to assist with creating HL7 Version 2, CDA, and FHIR security label implementation guidance for priority EHI security, privacy, and consent directives based on a consensus in support of TEFCA goals. In anticipation of this need, the HL7 Security and Community-Based Care and Privacy Work Groups have approved the development of a FHIR Data Segmentation for Privacy (DS4P) Implementation Guide (IG). For details, see the draft FHIR DS4P Project Scope Statement—https://confluence.hl7.org/display/SEC/FHIR+DS4P+IG+PSS?src=contextnavpagetreemode. The Work Groups have also approved a revision of the CDA DS4P IG to support a wider set of security, privacy, and consent directives.

QHIN Technical Framework (QTF) Draft 1 (Appendix 3)

The QTF and the Common Agreement

Comments:

- HL7 strongly supports ONC's proposal that, in a change from TEFCA Draft 1, the Qualified Health Information Network (QHIN) Technical Framework (QTF) would be incorporated by reference in the Common Agreement (CA) and finalized by and maintained by the RCE using an open, transparent and participatory governance process.

The QTF and Exchange Modalities

The Qualified Health Information Network (QHIN) Technical Framework (QTF) describes the functional and technical requirements that a Health Information Network needs to fulfill to serve as a QHIN under the Common Agreement. The QTF specifies the technical underpinnings for QHIN-to-QHIN exchange and other responsibilities described in the Common Agreement. The QTF focuses primarily on the technical and functional requirements for interoperability among QHINs, including specification of the standards QHINs must implement to enable QHIN-to-QHIN exchange of information. The technical and functional requirements described in the QTF enable the three information exchange modalities for QHINs expressed in the Common Agreement: QHIN Broadcast Query, QHIN Targeted Query, and QHIN Message Delivery.

Comments:

- ONC specifically focuses solely in the QTF on QHIN-to-QHIN exchange of information and specification of standards in the QTF only in relation to QHIN-to-QHIN exchange. HL7 agrees with TEFCA only specifying technical exchange standards at the level of QHIN-to-QHIN exchange and not seeking to dictate models of sub-QHN exchange beyond the applicable MRTCs.
- HL7 agrees with ONC that, "QHINs, Participants, and Participant Members are in no way limited from voluntarily offering additional exchange modalities and services or from entering into point-to-point or one-off agreements between organizations that are different from the Common Agreement's MRTCs, provided that such agreements do not conflict with the policies of the Common Agreement."

The QTF and HL7 Standards

The HL7 FHIR RESTful API is mentioned in the draft QHIN Technical Framework as Alternative/Emerging Standard or Profiles in the following places:

QHIN Exchange Network Query

- QHIN Query (HL7 FHIR RESTful API)
- QHIN Auditing (HL7 FHIR RESTful API)

QHIN Exchange Network Message Delivery

- Message Delivery (HL7 FHIR RESTful API)
- Auditing (HL7 FHIR RESTful API)

Query

- Query (HL7 FHIR RESTful API)

Message Delivery

- Message Delivery (HL7 FHIR RESTful API)

Auditing

- Auditing (HL7 FHIR RESTful API)

Comments:

- HL7 is pleased that ONC identifies the HL7® Fast Healthcare Interoperability Resources (FHIR®) RESTful API in the Qualified Health Information Network (QHIN) Technical Framework (QTF) Draft 1 as an Alternative/Emerging Standard or Profile in several critical areas. HL7 FHIR® is well positioned to support the collaborative use of FHIR-based standards as the QTF evolves and to help ensure that a patient's electronic health information (EHI) is accessible to a patient and the patient's designees, in a manner that facilitates communication with the patient, healthcare providers and other individuals.
- HL7 strongly emphasizes the importance and need of its implementation guides regarding the potential use of the HL7 FHIR RESTful API referenced in the QTF and in reference to the ONC QTF Request for Comment #6 that asks for insights on other appropriate standards to consider for implementation to enable more discrete data queries, such as emerging IHE profiles leveraging RESTful APIs and/or use of HL7

FHIR. Orderly, informed and fully successfully implementation of an HL7 standard or API is facilitated by implementation guides. If further HL7 implementation guide development is required in relation to the QTF, HL7 and its expert Work Groups stand ready to do so, given appropriate resources and to appropriately assist both ONC and the RCE.

User Authentication

SAML is an XML-based specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. The IHE XUA Profile leverages SAML to communicate claims about an authenticated entity in transactions that cross enterprise boundaries. The QTF Draft 1 specifies that QHINs implement IHE XUA to support exchange of authentication information among QHINs. Specified standards for User Authentication are included in Table 5.

Comments:

- HL7 notes that while the IHE XUA Profile leverages the OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) 1.0, the healthcare profile of SAML, which uses a hard-coded list of non-standard Purpose of Use codes and other non-standard codes, XUA's vocabulary is "open" such that implementers are free to update to the full set of HL7 Security Labels, including HL7 Purpose of Use codes found in XSPA 2.0
- XPSA 1.0 non-standard codes are problematic if used to adjudicate access requests for security labeled information tagged with the updated, standard HL7 Security Label vocabulary. This is the same vocabulary used to label HL7 Version 2, CDA, and FHIR content. They are also used in OAuth 2.0 profiles such as HEART and updates to SMART on FHIR to support clearance claims using json scope.
- The XSPA Technical Committee has published version 2.0 of XSPA Profile of SAML v2.0 for Healthcare Version. The new version is currently approved as a Committee Specification as announced by OASIS on 05/16/2019. The major updates in new version of XSPA profile of SAML are as the following:
    - Harmonizing with the latest versions of related standards, OASIS XACML and SAML;
    - Referencing HL7 vocabulary as the standard value sets for attributes such as purpose of use and security labels;
    - Providing non-normative guidelines for encoding XSPA attributes in JSON format to facilitate using these attributes in, or alongside, other protocols such as OAuth 2.0 and OpenID Connect;
    - Defining attributes required to support the Security Labeling System.

  Considering this update, HL7 recommends that the ONC and the RCE give serious consideration to having the QTF reference the latest version of the XSPA SAML profile (i.e. Version 2.0). This version provides a soft update to some of the existing attributes by considering them deprecated, but still valid in order to give vendors the flexibility of a gradual upgrade.
- Another consideration is that XSPA 2.0 supports security label vocabularies based on HL7 as they evolved over time, to meet emerging use cases. The XSPA SAML current Committee Draft is available to OASIS to members at SAML XSPA v2.0 Working Draft 14 (Membership is free) — http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html.

Query: RE XCPD and XCA for QHIN Query Obligations

ONC states that, with query today, many health information networks support queries for patient information maintained as clinical documents, such as care summaries formatted using the HL7 Clinical Document Architecture specification. IHE provides two widely implemented profiles supporting query-based, network-to-network document exchange: XCPD and XCA.

XCPD enables entities to locate communities that hold relevant patient health data and correlate patient identifiers across communities holding the same patient's data. XCA supports the means to query and retrieve relevant patient health data held by other communities in the form of documents. Using XCA requires knowledge of patient identity when querying for and retrieving clinical documents. Thus, XCA implementations often use XCPD to resolve identities across communities before making XCA requests. The QTF Draft 1 specifies that QHINs implement the IHE XCA and XCPD profiles to enable query-based network-to-network document exchange. These profiles satisfy a QHIN's obligations under the Common Agreement to initiate and respond to a QHIN Query.

Comments:

- HL7 agrees with the initial focus on mature IHE profiles (implemented through appropriate implementation guides and specifications as determined by the RCE). We also support identification of the Alternative/ Emerging Standard/Profiles, especially those based in HL7 FHIR as a migration path from the Specified Standard/Profiles listed in order to move toward a mixed ecosystem of legacy and emerging standards and technologies with clear signals about the exchange ecosystem envisioned for TEFCA.

ONC Request for Comment #2

What specific elements should a SAML assertion for User Authentication include?

Comments:

- HL7 recommends that ONC and the RCE evaluate a move, initially or in revisions to the QTF**,** to XSPA 2.0,

ONC Request for Comment #3

Should QHINs be required to transmit other authorization information (e.g., user roles, security labels) in addition to Exchange Purpose and any information required by IHE XUA? What specific elements should a SAML assertion include?"

Comments:

- See above comments on XSPA 2.0.
- HL7 notes that XSPA SAML 1.0, currently supported by IHE XUA, uses previous version hard-coded, non-standard purpose of use codes. This approach may be problematic if used to adjudicate access requests for security labeled information tagged with the updated, standard HL7 Purpose of Use codes. These are the same codes used to label HL7 Version 2, CDA, and FHIR content. They are also used in OAuth 2.0 profiles such as HEART and updates to SMART on FHIR to support clearance claims using json scope.

ONC Request for Comment #6

The IHE XCA profile is content-agnostic; it enables queries for documents based on metadata about the document but not the contents of the document itself. Therefore, the XCA profile does not necessarily support more granular queries for discrete data (e.g., a request for all clinical documents about a patient that contain a specific medication or laboratory result). Comments are requested on other appropriate standards to consider for implementation to enable more discrete data queries, such as emerging IHE profiles leveraging RESTful APIs and/or use of HL7 FHIR.

Comments:

- HL7 supports identification of the Alternative/Emerging Standard/Profiles, especially those based in HL7 FHIR as a migration path from the Specified Standard/Profiles listed in order to move toward a mixed ecosystem of legacy and emerging standards and technologies with clear signals about the exchange ecosystem envisioned for TEFCA.

ONC Request for Comment #7

The IHE XCPD profile only requires a minimal set of demographic information (i.e., name and birth date/time). Should QHINs use a broader set of specified patient demographic elements to resolve patient identity? What elements should comprise such a set?

Comments:

- HL7 recommends using a broader set of specified patient demographic elements to resolve patient identity especially given that with a wider demographic pool, the chances of mismatch will increase on a small number of elements. We recommend that ONC conduct further work to gain consensus on a broader set a of specified patient demographic elements and permit flexibility at the QHIN level to add additional matching parameters, as populations served may need an expanded list.

ONC Request for Comment #12

Future drafts of the QTF will specify a format for Meaningful Choice notices communicated between QHINs. Which standard/format should the QTF specify? What information should be included in a Meaningful Choice notice (e.g., should a notice include patient demographic information to enable QHINs to resolve the identity of the Individual that exercised Meaningful Choice)?

Comments:

- HL7 recommends that ONC include the elements from the FHIR Consent required for opting in and revocation. HL7 also recommends that ONC develop a standard user-friendly Meaningful Choice form based on the SDC FHIR Questionnaire/QuestionnaireResponse Resources, with computable transforms into a FHIR Consent for computable adjudication.

ONC Request for Comment #13

In addition to enabling Meaningful Choice, the Common Agreement requires QHINs to collect other information about an Individual's privacy preferences such as consent, approval, or other documentation when required by Applicable Law. Should the QTF specify a function to support the exchange of such information through the QHIN Exchange Network? Which standards and/or approaches should the QTF specify for this function?

Comments:

- HL7 recognizes that the type of information about an Individual's privacy preferences, such as consent, approval, or other documentation when required by Applicable Law runs a range of complexity in terms of legal compliance requirements and for computably adjudicating for access control. There is no one size fits all solution. HL7 possesses a CDA Consent Implementation Guide that could be used to address some of the more complex U.S. policies. HL7 has both the FHIR Consent and FHIR Contract to support different consent directive requirements and ONC goals and objectives here.