PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

June 17, 2019

Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Attention: TEFCA Draft 2
Mary E. Switzer Building, Mail Stop: 7033A
330 C Street SW, Washington, DC 20201

Dear Dr. Rucker,

Thank you for the opportunity to respond to the Trusted Exchange Framework and Common Agreement Draft 2. In the attached response, Partners HealthCare System, Inc. offers our thoughts on the newest version.

Sincerely,

James Noga,
Vice President & Chief Information Officer
Partners HealthCare, Inc.

INTRODUCTION

Partners HealthCare System, Inc. (“Partners”) is a Massachusetts-based, not-for-profit health care system that is committed to patient care, research, teaching, and service to the community locally and globally. Founded in 1994 by Brigham and Women's Hospital and Massachusetts General Hospital, Partners includes community and specialty hospitals, a managed care organization, a physician network, community health centers, home care and other health-related entities.

Several of our hospitals are teaching affiliates of Harvard Medical School, and Partners is a national leader in biomedical research.

We also recognize that increasing value and continuously improving quality of care are essential to maintaining excellence.

MINIMUM REQUIRED TERMS & CONDITIONS (MRTC'S)

Data Quality and Minimum Necessary

Partners agrees that the HIPAA minimum necessary requirement applies to EHI used or disclosed through the QHIN. Although HIPAA waives the minimum necessary requirement for treatment purposes, there are state and federal laws that require an individual's consent prior to use or disclosure, and these requirements would supersede the right to waive consent for treatment purposes. Examples of data uses or disclosures that would require patient consent even for treatment purposes include: HIV Test results, Genetic Screening Test Results, Alcohol and Drug Abuse Records, Sexual Assault or Domestic Violence Records, and certain mental health records. State-specific laws may require additional categories of information that require an individual's consent prior to use or disclosure.

Transparency

Partners believes that transparency between all parties involved in health information exchange is important and adequately covered in this section.

Cooperation and Non-Discrimination

Partners believes the requirements laid out in section 4 are essential to advancing health information exchange.

Privacy, Security and Patient Safety

Partners agrees with the majority of requirements outlined in this section. However, we do have a few specific comments below.

1. In section 6.1.1 on Breach Notification, we are concerned about the possibility of duplicate reporting on “suspected and known security incidents.” As currently written, the draft specifies that the QHIN is responsible for reporting any suspected security incidents to other QHIN's, Participants, Participant Members, and to Individuals with whom the QHIN has a direct relationship.   It is unclear which party would be responsible for notifying individuals with whom the QHIN doesn't have a direct relationship. Partners requests clarity around

reporting responsibilities and timeframes in order to establish accountability and avoid duplicate reporting for breaches.

2. As currently drafted in section 6.2.4, participants are required to provide identity proofing at a minimum of IAL2 or in accordance with policies. Partners maintains policies and procedures related to access control, which should be adequate and should apply to access credentials provided to staff being provided access credentials.
3. Lastly, in section 6.2.5, it should not be a requirement that QHIN staff and users are authenticated at a level of AAL2 or above. Authentication policy for QHIN staff and users should be commensurate with the QHIN policy for similarly classified applications and any step-up authentication, if deemed relevant, should be encouraged but not required.

Participant Minimum Obligations

Partners has concerns related to several of the subsection in Section 7: Participant Minimum Obligations. In section 7.3, as it seems to represent a major shift and limitation on the ability of Covered Entities to share EHI via the exchange for legally permissible purposes. If a participant can direct a Covered Entity not to share via the network EHI for otherwise permissible purposes, the inherent value and usefulness of the Exchange will be negatively impacted. In addition, we remain concerned that implementing such a requirement would be unduly burdensome and costly given the current technology landscape.

We request further detail on Section 7.4 which seems to conflict with the terms of Section 7.3. We request clarification on whether Covered Entities are permitted to disclose EHI via the Exchange for all legally permissible purposes. It is unclear if this is only allowed if an individual does not object or if affirmative consent is required in certain cases depending upon the requirements of Applicable Law.

We are concerned that the “information blocking” and “interoperability” provisions in Section 7.5 differ from the recently released CMS and ONC proposed rules on those issues making if unduly burdensome and costly for the QHIN and Participants to comply with a patchwork of information blocking prohibitions.

We would recommend that Section 7.12 be modified to clarify that the Participant’s obligation under this section relate solely to activities directly related to access to or information transmitted via the Exchange and would not apply more broadly to the information once it has been transmitted through the Exchange.

QUALIFIED HEALTH INFORMATION NETWORK (QHIN) TECHNICAL FRAMEWORK

ONC Request for Comment #1: Should the QTF specify additional standards or approaches for securing QHIN Exchange Network transactions (e.g. OASIS Web Services Security[47])?

Partners recommends complimenting TLS transport level security and integrity with a digital signature of the SAML assertion for message level security and integrity. We also recommend OWASP general SAML security best practices should be followed (https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SAML_Security_Cheat_Sheet.md)

ONC Request for Comment #2: What specific elements should a SAML assertion for User Authentication include?

We agree that Mutual authentication is necessary and that SAML and XUA should be used. Specific elements in the SAML assertion should include granular information about the client, entity and/or user.   We recommend providing any additional identifier for auditing purposes that would identify the user across the broader healthcare ecosystem. This identifier could be useful if\when a user moves across healthcare organizations and their identifier at the previous organization is either deleted or changed. NPI may be a good candidate.

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?

Partners recommends that OWASP general SAML security best practices should be followed. While SAML may technically be able to present authorization information by virtue of its XML foundation, it would be a proprietary implementation which this effort is looking to avoid. Partners encourages ONC to look at XACML or other related standards that target authorization and access control. We recommend that authorization information relevant to minimum necessary that is known to the QHIM and relevant to the Exchange Purpose should be passed in a normalized manner.

ONC Request for Comment #4: The Query function above describes a general workflow and set of capabilities for QHINs conducting query-based, inter-network document exchange. However, implementations may vary and result in divergence from the basic workflow. For example, a QHIN might fail to definitively resolve patient identity and consequently rely on a participant or Participant Member to determine the correct match. Likewise, Care quality's Query-Based Document Exchange Implementation Guide49 describes a number of alternate flows based on a "nominal flow." To inform subsequent work with the RCE to develop more specific technical guidance to address variation, comments are requested on the basic function presented and potential variations to consider.

We agree with the general workflow outlined in the QTF Query function. We also recognize several possible scenarios and variations of the workflows which couple implemented all parties in the exchange – first degree entities, initiating/responding GHINs, etc. The Alternate Flows and Error Flows described in Carequality's Query-Based Document Exchange Implementation Guide are extensive. These and possibly other flows should be addressed in the QTF. It is important to remove variability as much as possible to achieve a robust exchange network. We recognize that data may need to stored by the QHIN but we would be concerned with flows requiring data to be stored by other participants. We suggest avoiding this as much as possible.

Partners recommends establishing metadata requirements for the QHIN community for each of the Query functions described is critical to the success of the queries be it the standard workflow or the nominal flow.

ONC Request for Comment #5: The IHE XCA profile supports a number of defined queries (e.g., FindDocuments, GetAll, GetDocuments, GetRelatedDocuments, etc.). Each query includes a number of optional parameters. Should the QTF specify which queries/parameters a QHIN must support? Which queries/parameters are most widely implemented and/or useful today?

At this point in time the protocols chosen should be limited to those that service general purposes. The QTF should consider developing a Metadata Specification for the Community of QHINs that is defined by a collaboration of stakeholders. The guiding principles for this collaboration may be derived from the *IHE IT Infrastructure Handbook – Document Sharing Metadata Handbook.* Metadata is critical to data discovery and the attributes of value sets for certain parameters must be clearly defined. Decisions around supported Use Cases may guide what parameters beyond the 'critical few' are useful. The Use Cases should start with those most frequently deployed (i.e. Referrals, TOC, Consents) and as time goes on include the more specialized. Governance for the ongoing Metadata Specification is a requirement for success.

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.

The FHIR standard and adoption across the healthcare industry is evolving rapidly. We believe this will continue for several years as the standard matures and EHR vendors comply with the rules put forth by ONC and CMS. We support the inclusion of the FHIR standard in the QHIN Technical Framework but suggest that it align with requirements set forth in the ONC Proposed rule and not add any new requirements in terms of the supported version and/or resources. The burden on HIT Developers over the next few years will be significant and it would be beneficial to coordinate related efforts.

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?

Partners believes additional demographic elements are required to resolve patient identity. We recommend the addition of the following data element:

- Social Security Number;
- Mother's Maiden Name;
- Email address;
- Insurance policy number (when available);
- Other legal names patient may have used.

ONC Request for Comment #8: There are many possible approaches to Patient Identity Resolution, each with its own benefits and risks. For example, a centralized index of patient identity information may be more efficient for resolving patient identities across disparate communities, but also poses a greater risk to privacy if the system is compromised. Federated approaches may be less susceptible to external threats like cyberattacks, but harder to scale across many communities. Recognizing that new technologies and business entities with robust identity matching solutions may disrupt traditional approaches, should the QTF specify a single standardized approach to Patient Identity Resolution across QHINs?

We believe a single robust patient matching approach will be essential for patient matching. There should be a minimum data set that is collected for matching. In addition to the data demographic data standards, standards related to demographic content and frequency of updating demographic information should be established, for example use only legal name as it appears on government issued ID and verify or update patient demographics at each visit, or at least annually.

ONC Request for Comment #9: Different communities tolerate different degrees of risk with respect to accurately matching patient identities. Should QHINs meet a minimum performance standard (e.g., a minimum acceptable matching accuracy rate) over a specified time period? Likewise, different algorithmic techniques for matching patient identities use different approaches and must be tuned to the applicable patient population and continuously refined over time. Should QHINs measure and report on the performance of the algorithm(s) they rely on (e.g., by calculating precision, recall, etc.)?

We agree indicators on duplicate rate, duplicate creation rate and true match rate are important, however they are limited by the ability of the patient matching algorithm to accurately identify duplicate records. For example, one entity may show a low duplicate rate, however, it may be falsely low due to the failure of the algorithm to identity duplicates that another algorithm would identity. If these measures are to be useful to compare organizations, there needs to be a standard algorithm and standard definitions for the measures. EHRs should be required to meet the established minimum standard algorithm and be able to calculate and report on the standard metrics.

ONC Request for Comment #10: Recognizing there are different ways to implement Record Location services, should the QTF specify a single standardized approach across QHINs?

The QTF should specify a single methodology for RLS.

ONC Request for Comment #11: Should the QTF require QHINs to implement Directory Services? Recognizing there are many possible approaches for implementing Directory Services, should the QTF specify a single standardized approach? If QHINs implement Directory Services, which entities should be included in directories? Should directories be made publicly accessible?

Partners recommends that the QTF has a standardized approach for directory Service implementation and align the approach with the requirements set forth in the ONC Proposed rule and not add any new requirements or standards. Directory services have been difficult to support so it would be beneficial to coordinate related efforts.

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)?

QHINs must provide the same minimum identifiers specified for patient matching to ensure changes made based on Meaningful Choice are applied to the correct patient every time. If a Meaningful Choice notice does not contain the minimum identifiers, then it should not be accepted or acted upon. If applied to the incorrect patient the results could negatively impact the patient and overall trust in the system.

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?

Partners agrees that the QTF should specify a function to support individual's privacy preferences in order as well as require specific requirements for patient matching, as mentioned in #12.

ONC Request for Comment #14: QHINs may participate in a variety of activities and transactions involving First Degree Entities and/or internal operations, including receiving and processing Query and Message Delivery Solicitations, performing Patient Identity Resolution, performing Record Location, sending EHI, receiving EHI, performing queries, granting/revoking access credentials, etc. Future versions of the QTF may specify a list of events a QHIN must record involving First Degree Entities and/or internal operations. Which activities and transactions should the QTF specify as auditable events? What information should the QHIN record about each event?

Partners recommends that the QTF provide any additional identifier for auditing purposes that would identify the user across the broader healthcare ecosystem. This identifier could be useful if\when a user moves across healthcare organizations and their identifier at the previous organization is either deleted or changed.

We recommend the following auditable events include any attempt to access PHI or PII; any successful access of PHI or PII; any unrecognized actor. At a minimum the information that is audited should include date, time, transaction type, QHIN identifier, QHIN identity, user identifier(s), user identity, client IP and patient identifiers returned.

ONC Request for Comment #15: Should the QTF specify a consistent set of error messages for interactions between QHINS? Which error messages should the QTF specify? Should the QTF specify a consistent format for error messages

Partners believes that establishing a set of error messages and the definitions for those errors would benefit consumers. The community of QHINS should collaborate to establish a set of error messages and the format for these messages. Ongoing governance should be a part of the plan.