February 16, 2018

Dear ONC Team,

Thank you for the opportunity to provide feedback on the draft Trusted Exchange Framework and Common Agreement. I am excited about the clearly articulated principles that serve as the basis for this framework. Below, I'd like to share my detailed feedback on the draft TEFCA's technology and policy choices, including comments, questions, and fifteen specific recommendations, which I have prepared in my role as Visiting Scientist at Harvard Medical School. My recommendations focus on the scope and mechanics of individual access, including technical standards, security requirements, identity proofing, authentication, and authorization.

Sincerely,

Joshua Mandel, MD
Architect for SMART Health IT, Harvard Medical School Department of Biomedical Informatics
Health IT Ecosystem Lead, Verily

Standards Development and Recognition

2.4 states, "*within twelve (12) months of the date of the API Implementation Guide being formally adopted by HL7 on its public website and recognized by ONC on its public website.*" The framework should be designed to anticipate and accommodate the development of standards from a number of stakeholder organizations.For example, ONC may choose to recognize standards developed outside of the healthcare community for "generic" functionality like identity and access management.

Recommendation *1*: Do not exclusively list HL7 in this context. Instead, state that ONC will recognize API specifications and other standards for each selected use case.

Technical requirements for security

6.2.7 lists detailed technical restrictions without a clear statement about what these restrictions are intended to accomplish. Such details belong in an implementation guide with use cases, assumptions, preconditions, and specifications. Below, I'll highlight areas that contribute especially to my confusion.

6.2.7(i) and 6.2.7(ii) both describe "Authentication Server Requirements," but it's unclear what an "authentication server" is, especially in the context of FHIR APIs and OAuth as described in 6.2.7(i)(d).

6.2.7(ii)(b) states that "Each Qualified HIN shall authenticate third party applications to the authorization server's endpoint using a JSON Web Token (JWT) assertion signed by the third party application's private key as defined in RFC 7519." It's unclear what this requirement would mean or what problem it intends to address. RFC 7519 describes a general technology and not a specific authentication or authorization protocol. This level of detail about token formats is inappropriate outside the context of a dedicated implementation guide.

Recommendation *2*: Do not describe "authentication server requirements" inline, since an "authentication server" is not a well-defined concept. Instead, indicate that ONC will recognize specific security profiles for each selected use case.

6.2.7(iii) describes "Authorization Server Requirements." 6.2.7(iii)(a) appears to provide detailed rules about redirect URI comparison, but it's unclear what values are being compared, or when in the workflow this comparison would apply. This kind of detailed information does not belong in the TEFCA, since it is overly specific and lacks context. If needed, TEFCA should point to a comprehensive authorization profile for specific use cases (e.g., the authorization profile provided by SMART on FHIR). 6.2.7(iii)(c) refers to a "user information endpoint" which is not otherwise mentioned in the document. I can infer this is describing part of an OpenID Connect workflow, but it's unclear whether and how this relates to authorization. 6.2.7(iii)(d) refers to an end user's ability to revoke access tokens; but according to 6.2.7(iii)(b) these tokens have a short lifetime such that end-user revocation should be unnecessary. The focus should be on helping end users manage long-term access, and keeping access tokens short-lived enough that their revocation is irrelevant.

Recommendation *3*: Do not enumerate "authorization server requirements" directly in the document. Instead, indicate ONC will point to standard security profiles for the relevant use cases. Indicate that for individual-facing third-party apps, the SMART App Authorization Guide should apply. For other use cases, adopt or develop other specific guidance.

Individual Access and opt-out

Principle 5 indicates that QHINs should provide specific capabilities to individual patients, including a mechanism to access data and a mechanism to opt out of participation. It's unclear whether or how these capabilities would be offered in a real-world system. Three specific questions follow.

1. According to 3.1.9, QHINs have the capability to perform a "Brokered Broadcast Query" that fetches data about a given individual across a network of QHINs, as well as a "Directed Query" that fetches data from a more restricted list of participants. Are these capabilities available for individual patients to trigger, via any QHIN? In other words, can a patient instruct a QHIN to initiate a query for her own data across peer QHINs, just as a provider can do?

Recommendation *4*: Clarify that QHINS must enable individuals to initiate Brokered Broadcast Queries and Directed Queries for access to their own data.

2. According to Section 7.1, "a Qualified HIN shall not be required to include individuals as Participants or End Users." It is unclear how to reconcile this statement with the stated principle that individuals should have access to their own data. Perhaps the intent is that individuals would access specific QHINs using third-party apps that somehow become QHIN members? In this case, is the expectation that Individuals would still be able to sign into a QHIN for the purpose of approving this kind of third-party app? This interpretation seems to be supported by the Recommendation in 6.2.3(iv) indicating the use of SMART apps, and also by the details in 6.2.4(ii) indicating that "Each Qualified HIN shall identity proof individuals."

Recommendation *5*: Clarify the role of the QHIN, the individual, and a third-party app in the data-sharing workflow. Clarify that individuals must be able to sign into a QHIN for the purpose of approving a third-party application to access data. Given that individuals will have the ability to sign into a QHIN, individuals should also be able to trigger a query, and to view results directly from within the QHIN (i.e.,

analogous to the "View" objectives in Meaningful Use), rather than just approving access for a third-party app (i.e., analogous to the "Transmit" objectives in Meaningful Use).

Recommendation *6*: Remove the statement that "a Qualified HIN shall not be required to include individuals as Participants or End Users."

3. According to Principle 5(B), QHINs should "Have policies and procedures in place to allow a patient to withdraw or revoke his or her participation in the Qualified HIN." It is unclear how an individual would become aware of any given QHIN in order to opt out. Is there a plan to provide a centralized mechanism to facilitate global opt-out? If not, individuals may be unable to consistently express their opt-out preferences as new QHINs emerge.

Recommendation *7*: Provide an approach for global opt-out from the entire network of QHINs.

Section 6.1.1 states, "Similarly, each Qualified HIN agrees and acknowledges that individuals have a right to direct a Participant or End User to transmit a copy of EHI to any third parties designated by the individual in accordance with Applicable Law." This implies that participants and end-users, rather than the QHIN directly, are responsible for fulfilling individual access requests. But this model contradicts the expectations in 6.2.3-6.2.5, which state that QHINs should must support individual-facing applications according to the SMART App Authorization Guide. It also contradicts Principle 5(A), which states that "Qualified HINs ... should not limit third-party applications from accessing individuals' Electronic Health Information via an API."

Recommendation *8*: Clarify that when an individual approves a third-party app to access records within a QHIN, the QHIN is responsible for exposing an API to the third-party app, and that the QHIN API is responsible for performing the internal steps necessary to resolve queries (i.e., the QHIN is responsible for broadcasting brokered queries, aggregating the results, and returning them to the app). If this is inconsistent with ONC's regulatory intent, then clarify what is the intended purpose of enabling an individual to approve an app to access records within a QHIN.

Recommendation *9*: Clearly state that individuals must have the ability to sign into a QHIN in order to:

1. **Query across to network of QHINs for all data about themselves**
2. **Authorize apps of their choice to access their health care records via SMART on FHIR**
3. **Opt out of the QHIN ("Requests for No Data Exchange")**

Identity Proofing, Authentication, and Federated Authentication for Individuals

6.2.4(ii) states that "All personally identifiable information collected by the Participant staff or Qualified HIN shall be limited to the minimum necessary to resolve a unique identity." This is a confusing requirement, since participants will often maintain long-term relationships with individuals and will want to collect data for purposes that go far beyond unique identity resolution. For example, a clinic may want to collect a patient's mobile phone number or work address, even if they have already resolved a unique identity without these data.

Recommendation *10*: Remove the statement "All personally identifiable information... shall be limited to the minimum necessary to resolve a unique identity."

6.2.5(i) states that "Each Qualified HIN shall ... provide support for at least FAL2 or, alternatively, FAL3." It is

unclear whether "provide support for at least FAL" means that the QHIN needs to act as a federated identity provider (IDP), or to act as a federated relying party (RP). The most important need is to ensure that consumers can sign into healthcare record systems using their preferred identity providers. In other words, QHINs should be capable of acting as relying parties to consumer-selected identity providers. Consumers who want it should have the option to "Sign in with Facebook / Google / Microsoft" and so on.

Recommendation *11*: Clarify that the intention is for QHINs to act as relying parties in federated identity workflows that support individual access.

Given Recommendation 11, two questions remain:

1. *Which IDPs must be supported?* Are there particular federated IDPs that the QHIN would need to support? Or is the proposed requirement that each QHIN would need to "provide support" for at least one federated IDP? Or that a given QHIN would need to "provide support" for every federated IDP that meets the required FAL bar?

   Recommendation *12*: Clarify that QHINs may choose which federated identity providers they support, but that each QHIN must support at least one federated identity provider and must list all supported providers in public-facing documentation.

   Recommendation *13*: Encourage QHINs to support federated identity providers that are widely adopted by the individuals who use the QHIN.

2. *What FAL should be required?* The proposal appears to prohibit QHINs from relying on federated IDPs at FAL1. This would prevent patients from signing in using OpenID Connect implementations from federated identities that are widely available to and used by individuals today (e.g. Facebook, Google, Microsoft), since these services do not support audience-specific encryption of id_tokens. However, if QHINs issue an appropriately scoped request to these IDPs, they can obtain an id_token that omits personal identifiers and conveys only a "subject" claim. https://pages.nist.gov/800-63-3/sp800-63-3.html#-63-selecting-fal indicates that when an assertion does not include personal data (as would be the case for an id_token that conveys only a subject id), then FAL1 may be appropriate. Overall, FAL2 imposes very severe limitation on the federation ecosystem without delivering any obvious value.

   Recommendation *14*: Adopt FAL1 as the appropriate minimum bar for individuals who use a federated identity to sign into their healthcare provider systems.

To support key use cases of individual access and opt-out, individuals must be able to sign into QHINs. Does a patient need to have a relationship with a healthcare provider within a QHIN before creating an account at the QHIN? If yes, how does proactive opt-out work? If no, then who sets expectations for identity proofing and who adjudicates matches in the case of uncertainty?

Recommendation *15*: Clarify that individuals do <u>not</u> need a relationship with any particular health care provider before they are able to sign into a QHIN. Clarify that QHINs are responsible for adequately identity proofing individuals through an online workflow in the case that participants have not already worked with a health care provider to establish identity.