patientprivacyrights

QHIN Technical Framework PPR Comment

Do the draft regulations allow a QHIN to compete on privacy? Competition on privacy in the context of TEFCA means that a QHIN could solicit business by offering Individuals more transparency and more control over how their personal information is shared with other parties including other QHINs. We believe the ability to compete on privacy is essential to achieving the three goals of TEFCA:

1. Provide a single "on-ramp" to nationwide connectivity
2. Electronic Health Information (EHI) securely follows you when and where it is needed
3. Support nationwide scalability

We interpret the goals to apply to individual patients or physicians. Some patients and some physicians, such as psychiatrists, are much more privacy-sensitive than others. In order to participate in TEFCA, privacy-sensitive users might reasonably require:

- Strict control over the specific recipients of information (similar to 42CFR Part 2 rules)
- Notice of all instances of PII access by anyone for any reason, including TPO
- A single point of contact to review an accounting for disclosures
- The ability to decide which relationships are discoverable in a Broadcast Query
- The ability to host and operate their own authorization server to avoid sharing policies with a QHIN.
- The ability to interact directly with a chosen QHIN as a fiduciary, might also be essential

Page 73 - "The SAML assertion includes information about the provider's identity and the Exchange Purpose."
Good - This enables the Responding QHIN to send this information to a patient's authorization server.

Page 73 - "Each Responding QHIN uses the demographic information to resolve the patient's identity (i.e., "patient matching"), and returns an XCPD response with the resolved identity (including a local patient identifier, demographic information about the patient, information about providers that have seen the patient, etc.)."
Careful - The Responding QHIN must only match against parameters that are explicitly provided by the patient. For example, the patient might provide a Name and email address to the responding QHIN. If that's a match, then the process proceeds. If it's not, then the Responding QHIN stays silent.

Page 73 - "After retrieving the relevant documents, the Initiating QHIN transmits them back to the HIE that submitted the Query Solicitation, which then transmits them to the provider."
Careful - This can work but it should be clear that end-to-end encryption is supported so that the QHINs don't have to have access to the contents of the message. For example, the provider's

identity could be linked to a public encryption key. The source of the document (as discovered via the relationship locator service) can use the provider's identity to fetch their public key and use that to encrypt the response. This avoids snooping by the TEFCA intermediaries.

Pages 74 and 75 - "recipient of the message (may be known by the sender or obtained via a query transaction)."
Careful - Note that the recipient of the message might be a physician selected by the patient because they have a secure identity (possibly linked to Direct) and an associated public key that would allow end-to-end encryption of the message. We should not design TEFCA in any way that prevents end-to-end encryption.

Page 75 - "*Note:* Message Delivery on behalf of a patient (i.e., Individual User) for the Individual Access Services Exchange Purpose follows a similar workflow. For example, a patient may direct their provider to send EHI to a mobile application or another provider. Likewise, First Degree Entities may also initiate a Message Delivery Solicitation."
Important - This is another reason to support end-to-end encryption. Some mobile applications that are not otherwise TEFCA-aware might just wish to support end-to-end encryption with the patient in control of the keys.

Page 79 - "** ONC Request for Comment #2: What specific elements should a SAML assertion for User Authentication include?"*
Important - TEFCA should not dilute the right of patients under HIPAA to be "known to the practice". A patient can have a secure voluntary identity at a participant without being identity proofed by the practice. In that case, it is up to the patient when seen at another practice to prove to the other practice that they are in control of the identity at the practice they are communicating with. This is commonly done with the OAuth protocol which is already well established for FHIR and SMART on FHIR. Simply put, with OAuth, the patient proves they are the same person by signing in to the patient portal of both practices. No identity proofing is necessary because the patient can be "known to the practice" separately on both ends of the sharing transaction. TEFCA should be careful not to dilute HIPAA in this major way.

Page 80 - "** 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?"*
Important - To support competition for privacy by QHINs, TEFCA should not force patients to share their authorization policies with a QHIN that is willing to support a patient's UMA (also HEART Workgroup) authorization server. An UMA-aware QHIN can simply pass the authorization information, no matter how they received it, to the patient specified UMA Authorization Server.

Page 82 - "However, a sender may not know a recipient's Direct address or may not use Direct. In such cases, the QHIN Exchange Network provides a complementary set of Message Delivery capabilities."

Careful - The goal of “a single on-ramp” should apply to patients as well as physicians and institutions. TEFCA should make every effort to support secure end-to-end encrypted messages and queries. This will enable TEFCA to be fully used by patients via mobile apps as long as they can find an appropriate QHIN that wants their business.

Signed,

Adrian Gropper, MD
CTO, Patient Privacy Rights

Deborah C. Peel, MD
Founder and President, Patient Privacy Rights