The Office of the National Coordinator for Health Information Technology

Health IT Advisory Committee

Trusted Exchange Framework and Common Agreement (TEFCA) Task Force

Arien Malec, Co-Chair
John Kansky, Co-Chair

May 23, 2019

Agenda

- Call to Order/Roll Call
- Continue Privacy Discussion
- Begin Security Discussion
- Public Comment
- Next Steps and Adjourn

Task Force Charge

- **Overarching charge:** The Trusted Exchange Framework and Common Agreement (TEFCA) Task Force will develop and advance recommendations on the TEFCA Draft 2 to inform development of the final Common Agreement.
- **Detailed charge:** Make specific recommendations on the Minimum Required Terms and Conditions and the Qualified Health Information Network (QHIN) Technical Framework (QTF) —
  - **Definition, Structure, and Application Process for QHINs:** Recommendations for further clarifying the eligibility requirements and application process for becoming a QHIN.
  - **Exchange Purposes and Modalities:** Recommendations on enhancing or clarifying the seven (7) exchange purposes and three (3) exchange modalities proposed in the MRTCs, as well as provisions regarding EHI reciprocity and permitted and future uses of EHI.
  - **Privacy:** Recommendations on privacy requirements for participating entities, including Meaningful Choice, Written Privacy Summary, Summary of Disclosures, and Breach Notifications
  - **Security:** Recommendations on security requirements for participating entities, including minimum security requirements, identity proofing, authorization, and authentication.

The Office of the National Coordinator for Health Information Technology

Privacy

@ONC_HealthIT @HHSONC HealthIT.gov

Minimum Information

Minimum Information: all of the following information in plain language and in a conspicuous format that must be received by an Individual before he or she grants the approval required under Section 2.2.2, Section 7.2 or Section 8.2 below:

- the person or entity that will be taking such action;
- the specific purpose(s) for which such action may be taken;
- how long such action may be taken;
- whether EHI may be Disclosed to any third party (and, if so, to whom and for what purpose);
- whether EHI may be Used by a third party (and, if so, identifying the third party and the Uses);
- whether the QHIN, Participant, Participant Member, and any third party to which any of them may Disclose the EHI (including any agents or subcontractors of any of them) are required to comply with the HIPAA Rules;
- whether EHI may be sold or licensed;
- any material benefits or risks of such action; and
- whether the privacy and security measures set forth in the MRTCs will apply to the EHI that is the subject of such action (including whether they will apply to any recipient of the EHI).

For purposes of this definition, information in all capital letters shall not be used to satisfy the requirement that the Minimum Information be conspicuous.

Privacy Requirements

- **Breach Notification Requirements (6.1.1, 6.1.2, 7.12, 7.13, 8.12, 8.13)—**Included requirement 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 or not they are a Covered Entity or Business Associate. Further, each QHIN shall notify the RCE, as well as other QHINs, Participants, Participant Members, and Individual Users who may have been affected by the Breach without unreasonable delay and in accordance with Applicable Law.
- **Meaningful Choice (2.2.3, 7.3, 8.3)—**QHINs, Participants, and Participant Members must provide Individuals with whom they have a Direct Relationship 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 up to the QHIN who must then communicate the choice to all other QHINs.
- **Minimum Necessary (3.3, 7.19, 8.19)—**QHINs, Participants, and Participant Members shall satisfy the Minimum Necessary Requirements at 45 CFR § 164.514(d) as if they applied to EHI.

Privacy, continued

- **Other Legal Requirements (6.1.4, 7.4, 8.4)—**QHINs, Participants, and Participant Members with a Direct Relationship with an Individual shall obtain and maintain copies of the Individual's consent, approval or other documentation when required by Applicable Law. The participating entity may make it available electronically to any other Participant, QHIN, or Participant Member upon request to the extent permitted by Applicable Law.
- **Written Privacy Summary (6.1.5, 7.6, 8.6)—**QHINs, Participants, and Participant Members 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 explaining how an Individual can exercise their Meaningful Choice and who they may contact for more information about the entity's privacy practices.
- **Summary of Disclosures (6.1.6, 7.20, 8.20, 9.5)—**Individuals shall have the right to receive a summary of Disclosures of EHI for applicable Exchange Purposes in the context of the Framework Agreements for up to a period of six (6) years immediately prior to the date on which the summary of Disclosures is requested. For Covered Entities, this obligation may be met by complying with the requirements of 45 CFR § 164.528.

The Office of the National Coordinator for Health Information Technology

Security

@ONC_HealthIT @HHSONC HealthIT.gov

Security Requirements

- **Minimum Security Requirements (6.2, 7.7, 8.7)—**All QHINs shall comply with the HIPAA Privacy and Security Rules as if they applied to EHI. Participants and Participant Members must comply with the HIPAA Rules when applicable. However, regardless of whether they are a Covered Entity or Business Associate, Participants and Participant Members must take reasonable steps to promote the confidentiality, integrity, and availability of EHI.
- **NIST SP 800-171 (6.2.1)—**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).
- **No EHI Used or Disclosed outside the US (2.2.11)—**QHINs shall not Use or Disclose EHI outside the US, except as required by Applicable Law and to the extent an Individual User requires their EHI to be Used or Disclosed outside the US. QHINs may only utilize cloud-based services that are physically located within the US.

Security, continued

- **Data Integrity (6.2.2, 7.16, 8.16)—**QHINs, Participants, and Participant Members shall include procedures to promote data integrity with respect to the Exchange Purposes it performs.
- **Authorization (6.2.3, 7.8, 8.8)—**QHINs, Participants, and Participant Members 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., granted and provisioned in security and privacy management).
- **Identity Proofing (6.2.4, 7.9, 8.9)—**QHINS, Participants, and Participant Members shall be identity proofed at a minimum of IAL 2 and require proof of identity for Individual Users at a minimum of IAL2 prior to issuance of credentials.

Security, continued

- **User Authentication (6.2.5, 7.10, 8.10)—**QHINS, Participants, and Participant Members shall be authenticated at AAL2 (with support for FAL2) and require Individual Users be authenticated at a minimum of AAL2 prior to issuance of credentials.
- **Transport Security (6.2.6, 7.17, 8.17)—**QHINs, Participants, and Participant Members' security policies shall include written policies and procedures to ensure a secure channel for communications between Participants and QHINs and between Participants and Participant Members.
- **Auditable Events (6.2.8, 7.11, 8.11)—**QHINs, Participants, and Participant Members shall abide by the auditable events requirements described in the QHIN Technical Framework with respect to the Exchange Purposes it performs.

Security, continued

- **Certificate Policies (6.2.7)—**Each QHIN's security policy shall require that all Participant cryptographic certificates meet or exceed the applicable criteria in the QHIN Technical Framework.
- **Certificate Authority Backup and Recovery (6.2.9)—**Each QHIN who is an issuer of certificates shall maintain backup copies of system, databases, and private keys in order to rebuild the certificate authorities' capability in the event of software and/or data corruption.
- **Security Labeling (Introduction)—**ONC requests comment on inclusion of a new requirement regarding the use of confidentiality codes and security tags and/or reasonable alternatives that would ultimately promote the ability to exchange sensitive data under the Common Agreement.

Public Comment

To make a comment please call:

Dial: 1-877-407-7192

*(once connected, press "*1" to speak)*

All public comments will be limited to three minutes.

You may enter a comment in the
"Public Comment" field below this presentation.

Or, email your public comment to onc-hitac@accelsolutionsllc.com.

Written comments will not be read at this time, but they will be delivered to members of the Workgroup and made part of the Public Record.

Meeting Adjourned