Meeting Notes

Health Information Technology Advisory Committee
Trusted Exchange Framework and Common Agreement Task Force
May 23, 2019, 12:00 p.m. – 1:30 p.m. ET
Virtual

The May 23, 2019, meeting of the Trusted Exchange Framework and Common Agreement (TEFCA) Taskforce of the Health IT Advisory Committee (HITAC) was called to order at 12:00 p.m. ET by Cassandra Hadley, Designated Federal Officer, Office of the National Coordinator for Health IT (ONC).

Cassandra Hadley conducted roll.

Roll Call

Arien Malec, Co-Chair, Change Healthcare
John Kansky, Co-Chair, Indiana Health Information Exchange
Laura Conn, Centers for Disease Control and Prevention
Cynthia A. Fisher, WaterRev, LLC
David McCallie, Cerner
Aaron Miri, The University of Texas at Austin, Dell Medical School, and UT Health Austin
Carolyn Petersen, Individual
Mark Savage, UCSF Center for Digital Health Innovation
Sasha TerMaat, Epic
Grace Terrell, Envision Genomics, Inc.
Sheryl Turney, Anthem Blue Cross Blue Shield

MEMBERS NOT IN ATTENDANCE

Noam Arzt, HLN Consulting
Anil Jain, IBM Watson Health
Mark Roche, CMS
Steve L. Ready, Norton Healthcare
Andrew Truscott, Accenture
Denise Webb, Individual

ONC STAFF

Zoe Barber, Staff Lead
Michael Berry, SME
Cassandra Hadley, HITAC Back Up/Support
Alex Kontur, SME
Kathryn Marchesini, Chief Privacy Officer, ONC
Kim Tavernia, SME

Call to Order

Cassandra Hadley called the meeting to order and turned the meeting over to Arien Malec, co-chair.

Arien Malec welcomed the members and noted that progress for the Trusted Exchange Framework and Common Agreement (TEFCA) task force has been somewhat slow and this is primarily due to other activities, including the Information Blocking Task Force and HITAC meetings. He suggested that the TEFCA Task Force is now poised for faster progress, but that the ability of the task force to make recommendations to ONC prior to the close of the comment period is at risk, and an extension request may be necessary. He then noted that to ensure overall progress, the goals for the current meeting is to discuss the items noted on the agenda and within the presentation and each member can indicate if they'd like to discuss in detail during a subsequent deep-dive session. He also clarified that in the meeting to follow the current meeting, the task force would prioritize the work of the task force against the highest priority needs that require comment.

John Kansky further clarified the goal of the current meeting and asked the task force members to raise their hands to note the subjects they'd like to discuss in detail in subsequent meetings.

Continue Privacy Discussion

Zoe Barber began the presentation by discussing privacy considerations.

Privacy Slide

Zoe Barber noted that the privacy and security section was drafted in a way to align with and complement applicable law, particularly the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules as much as possible. She commented that currently, minimum required terms and conditions (MRTC) are written with the assumption that everybody who is a covered entity, or a business associate is currently following the HIPAA privacy and security rules. She noted that in this section, qualified health information network (QHIN) must comply with the HIPAA privacy and security rules as if it applies to all electronic health information (EHI). She also noted that there is an exception for federal agencies, (e.g., Social Security Administration) who currently do not have to follow HIPAA as they are following their own applicable laws.

- **Arien Malec** commented that his understanding is that in most cases, a health information network (HIN) or QHIN would already be a business associate and already be transacting data on behalf of the covered entity, in those cases, compliance with HIPAA would be required. He went on to note that there are cases where a HIN may be transacting data on behalf of a noncovered entity, and the intent of structuring it the way the TEF does is to make sure there is no ambiguity and that everybody is basically holding against the same baseline rules.
- **Zoe Barber** agreed with Arien's understanding and noted the overall goal being sought is to achieve the right balance between protecting the privacy and security of the information that flows through the network but still expanding access.
- **John Kansky** sought confirmation from Zoe on his understanding that it is to comply with the HIPAA rules called out as if they apply to EHI.
    - **Zoe Barber** confirmed this.

- **David McCallie** commented that he believes that some of the entities that would like to participate in the ecosystem would currently be regulated under the Federal Trade Commission (FTC) rules, and the industry has adopted this sort of notion that either you are under HIPAA or under FTC, and depending on which, the rules are different. He noted that it would be useful to clarify those boundary conditions. Zoe agreed, and this question was added to the list to discuss in detail in the subsequent meeting.
- **Mark Savage** referred back to Arien's comment regarding HIN's, and QHIN's already being considered business associates and suggested the task force consider situations where there may not be a relationship and the entity must act as-if HIPAA applies. He then noted that there are some differences between covered entities and business associates and asked in what role they have to act.
    - **Arien Malec** answered that they have to act according to HIPAA provisions that apply to QHINs, independent of their status. He noted that the task force will discuss those provisions shortly.
- **Arien Malec** sought confirmation from Zoe that this is not preemptive. He clarified that a covered entity or business associate already covered by the covered entity terms, that those terms still apply. He further clarified that his focus is on the cases where nothing else applies.
    - **Zoe Barber** confirmed this and went on to explain that it does not supplant an entities requirement to, for example, do a notice of privacy practices. However, she noted that there are instances where satisfying the requirement through HIPAA can serve as satisfying the requirement from the MRTCs. Finally, she noted that this will be discussed further in this and subsequent meetings.

Minimum Information Slide

- **David McCallie** asked to whom the minimum information provisions apply, and when must they be provided to the individual.
    - **Zoe Barber** answered consent from the individual who is the subject of the information that received by either the QHIN participant or participant member is required for anything they want to do with the data that is not one of the exchange purposes listed in the MRTC.
- **John Kansky** sought clarification on if the minimum information provisions being discussed gave authority for anything legal to be done with the data as long as the consumer agreed to it or if they could do anything with the data that is not illegal without consumer consent.
    - **Zoe Barber** answered that anything could be done that is covered by applicable law.
    - **Kathryn Marchesini** added that the intent was to focus and standardize the areas deemed most problematic.
    - **Arien Malec** noted that there might be boundary positions where a company may act in one role in a given circumstance and then act in another role in other circumstances and asked at which point are they operating under the TEF subject to these rules and in which point are they acting purely on behalf of the individual?
    - **David McCallie** asked if an individual chose to use the APIs required under the data blocking rule, and downloaded their data directly from a provider, how do the constraints of that access channel to my data differ from access channel to my data through TEF?
    - **Zoe Barber** suggested noting the questions and concerns for detailed discussion at a later time and continued the presentation.

Privacy Requirements Slide

- **David McCallie** asked when meaningful choice might not apply. For example, is direct treatment clearly called out an exemption, or does this actually change with the rules?
    - **Zoe Barber** answered that it is not called out as an exemption. Unless, for example, not exchanging it would be a violation of the law, there are currently no other exceptions to meaningful choice.
- **Arien Malec** sought confirmation on the intent, which he understood to mean that QHIN's must make sure participants let their patients know that they are participating, help them understand what that participation includes, and give them the opportunity to participate or not, based on the information provided.
    - **Zoe Barber** confirmed that this matches her understanding of the intent but sought input on perfecting the language and intent.
- **Mark Savage** asked that if someone is exercising meaningful choice with direct treatment but not QHIN Technical Framework (QTF).
    - **Zoe Barber** answered that it applies to the common agreement as a whole.
    - **David McCallie** noted that he felt it was unclear as to the boundaries to what someone could meaningfully opt-out for sharing regarding direct treatment. He then noted that sharing the privacy preferences of an individual's meaningful choice action across a network is not a very well solved technical problem. This concern was added to the list for deeper discussion at a later time.
- Regarding meaningful choice, **Arron Miri** asked if when a patient opts out, do they opt out of everything or can they actually opt out of the way the data is being used.
    - **Zoe Barber** answered that the way it's currently written, the opt-out is all-or-nothing.
- **Aron Miri** then asked that regarding breach notification, it's possible that QHIN's could reside in different states with variable rules on breach timing. He went on to ask if this is this replacing the need for individual QHINs to know their local laws as well?
    - **Zoe Barber** answered that no, applicable law includes all local state and federal law.
- Related to mental health and substance abuse **Aron Miri** wondered how these are differentiated when it comes to meaningful choice**.** He asked if there is a granular level of consent that needs to be given as it relates to these subjects, or is it all or nothing?
    - **Zoe Barber** answered that as it stands, it is all or nothing. She added the caveat that they are asking for recommendations and comments around standards or security tagging and confidentiality codes. This concern was added to the list for deeper discussion at a later time.
- **Mark Savage** asked if the individual exercises meaningful choice somewhere midway and there is already some data being exchanged, is this draft clear about what happens with the data that's already in the system?
    - **Zoe Barber** answered that meaningful choice is only on a prospective basis. She added that anything that's already been used or disclosed prior to the exercise of meaningful choice can continue to be used or disclosed.

Privacy Slide Continued

- **Arien Malec** and **David McCallie** asked if the accounting disclosure or summary disclosures apply to the activities of the organization to which the patient has a direct relationship and any QHIN that that organization may participate with? Or does that summary of disclosures relate to any activity of any QHIN that is participating in the TEF? This concern was added to the list for deeper discussion.

- **David McCallie** referred to the summary of disclosures for applicable exchange purposes, and asked if it is the same thing one would account for disclosures for under HIPAA or all exchange purposes transaction period?
    - **Zoe Barber** answered the applicable exchange purposes that are relevant in the MRTC. She further noted there was an exception for Treatment, Payment, and Health Care Operations (TPO). Zoe then displayed the pertinent language on the screen and noted that section 9.5.3 has all the exceptions.
    - **David McCallie** noted that he understood that the goal was not to supplant the need for a HIPAA notice of privacy practices, and asked if this means that every covered entity that participates in the TEFCA ecosystem is going to have two privacy notices?
    - **Zoe Barber** answered that it could mean that they could just modify it to make sure it serves both purposes.

Begin Security Discussion

Alex Kontur continued the presentation previously led by Zoe by discussing security considerations.

Privacy Requirements Slides

- **Arien Malec** asked how or if the task force should align federal agency requirements related to QHIN requirements. This concern was added to the list for deeper discussion.
- Regarding "No EHI Used or Disclosed outside the US (2.2.11)," **Arien Malec** asked why this provision is particular to cloud-based service providers. He further asked if a hosting facility can be located outside the US. This concern and a suggestion that the term 'cloud-based' is clarified was added to the list for deeper discussion.
- **David McCallie** noted that much of the security provisions covered overlapped with existing HIPAA security and asked what the intent was.
    - **Zoe Barber** answered that unlike HIPAA it applies to all electronic health information, but otherwise it does mirror what is in HIPAA. She added that it only applies to processes for the exchange purposes that are an entity performs. She added that participant members if they are not covered entities and business associates, do not have to comply with all of HIPAA. They only have to comply with the provisions as explicitly laid out.
- **David McCallie** asked if the 'Transport Security' provision and the 'Auditable Events' provision introduce new burdens compared to what participants in, for example, CommonWell and Carequality are already doing?
- Referring to the User Authentication provision, **Arien Malec** suggested he was confused by National Institute of Standards and Technology (NIST) level II, and noted he thought NIST went to a changed terminology in later guidance. And this is specific identity insurance and not authentication. He then suggested they refer to the exact sections in the guidance.

  - **Alex Kontur** answered that they refer only to the guidance overall rather than specific sections. Alex also confirmed that AAL2 refers to authentication (IAL is identity proofing).
  - **John Kansky** sought confirmation that participants can accept the identity proofing of a participant member, and the QHIN can accept identity proofing of participants.
  - **Zoe Barber** confirmed this and **Arien Malec** clarified that as long as identity proofing is authenticated at the appropriate level. He went on to note that IAL2 is real world identify proofing and AAL2 is two-factor authentication.
- **Arien Malec** suggested flagging the Auditable Events provision for further discussion and noted the reason is that he felt it was odd to have MRTCs that refer to QTF that will change.
- Referring to the Auditable Events provision, **David McCallie** related this to the accounting for disclosure requirements and sought clarity that this was auditable by who and under what circumstances.
- **Alex Kontur** answered that there is language outlining that the entities must maintain an audit log, including records of all these events and must make it available to any audit but noted that who is doing the audits is not specified. This concern was added to the list for deeper discussion at a later time.
- Referring to the Certificate Policies Provision, **Arien Malec** noted that they covered individual identity assurance, but not organizational identity assurance and asked if the MRTC's discuss organizational identity assurance.
  - **Alex Kontur** noted that he believed that the NIST specification applies to both. This concern was added to the list for deeper discussion at a later time.
- Referring to the Certificate Authority Backup and Recovery provision **Arien Malec** commented that it was extraordinarily bad practice to include this and flagged this issue to be added to the list for deeper discussion at a later time.
- **David McCallie** referred to security labeling and sought clarification on if this is preamble, but not part of the actual MRTCs. He went on to ask if that means it would be deferred to the Recognized Coordinating Entity (RCE) to work out with ONC in the future?
  - **Alex Kontur** answered that based on comments that they get, this might be incorporated into a future version of the MRTCs, so that wouldn't necessarily involve the RCE establishing a policy, but rather ONC establishing a policy. He went on to note that the proposed policies do not make mention of controlled unclassified information (CUI) and suggested adding this issue to the list for deeper discussion.

Cassandra Hadley opened the lines for public comment.

Public Comment

There were no public comments.

Comments in the Public Chat

Mark Segal: Given 6.1.1, is the intention that all HIPAA privacy requirements apply, not just those for breach: "6.1.1 Breach Notification Requirements and Security Incidents. Each QHIN shall comply with the HIPAA Rules as if they apply to EHI, including but not limited to the Breach notification requirements applicable to Business Associates pursuant to 45 CFR Part 164 Subpart D regardless of whether it is a

Business Associate; provided, however, that if the QHIN is a Covered Entity, it shall comply with the Breach reporting requirements that apply to Covered Entities in addition to providing the notices required below.".

Next Steps and Adjourn

After public comment, **Arien Malec** suggested adjourning the meeting early and assembling a list of the high priority topics for later discussion.

Discussion Topics Notes

- Boundary discussion which actors are under HIPAA and which actors are under FTC
- Understanding when provisions apply for sharing/using consumer data
- Direct treatment examples as related to meaningful choice
- Discuss SUD/OUD as related to meaningful choice
- What is "prospective" as related to meaningful choice
- Flow of Summary of Disclosures and what entities do they apply to
- How to align federal agency security requirements related to QHIN security requirements
- Can cloud based services be hosted outside US
- Comments as to if identity proofing/authentication is disruptive to existing practices
- Auditable events, QTFs will change so discuss how requirements can be chosen
- Which entity will be performing the audits of auditable events
- Certificate policies for organizational identity assurance
- Certificate authority backup and recovery 6.2.9 flagged for discussion of removal

Cassandra Hadley adjourned the meeting at 1:30 p.m. ET