Meeting Notes

Health Information Technology Advisory Committee
Trusted Exchange Framework Task Force
June 4, 2019, 1:00 p.m. – 2:30 p.m. ET
Virtual

The June 4, 2019, meeting of the Trusted Exchange Framework and Common Agreement (TEFCA) Taskforce (TF) of the Health IT Advisory Committee (HITAC) was called to order at 1:00 p.m. ET by Lauren Richie, Designated Federal Officer, Office of the National Coordinator for Health IT (ONC).

Lauren Richie conducted roll.

Roll Call

John Kansky, Co-Chair, Indiana Health Information Exchange
Noam Arzt, HLN Consulting
Anil Jain, IBM Watson Health
David McCallie, Jr., Individual
Carolyn Petersen, Individual
Mark Savage, National Partnership for Women & Families
Sasha TerMaat, Epic
Andrew Truscott, Accenture
Sheryl Turney, Anthem Blue Cross Blue Shield
Denise Webb, Individual

MEMBERS NOT IN ATTENDANCE

Arien Malec, Co-Chair, Change Healthcare
Cynthia A. Fisher, WaterRev, LLC
Aaron Miri, The University of Texas at Austin, Dell Medical School, and UT Health Austin
Steve L. Ready, Norton Healthcare
Mark Roche, Federal Representative, Centers for Medicare and Medicaid Services (CMS)
Grace Terrell, Envision Genomics, Inc

FEDERAL REPRESENTATIVE

Laura Conn, Federal Representative, Centers for Disease Control and Prevention

ONC STAFF

Zoe Barber, Staff Lead
Michael Berry, SME
Cassandra Hadley, HITAC Back Up/Support
Alex Kontur, SME

Kathryn Marchesini, Chief Privacy Officer
Lauren Richie, Branch Chief, Coordination, Designated Federal Officer
Kim Tavernia, SME

Lauren Richie turned the meeting over to John Kansky, co-chair, and Zoe Barber.

Zoe Barber introduced Jonathan Coleman, who is a security consultant and will be participating in the discussion to answer any security questions that may arise.

John Kansky reviewed the agenda, noting that the goal is to finish walking through the matrix. He noted his appreciation for Jonathan Coleman's participation, as much of today's discussion will focus on security.

Discussion on Security Provisions

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

John Kansky began the discussion with controlled unclassified information (CUI) in the matrix.

- **David McCallie** asked Johnathan Coleman if he had a good summary of what CUI inclusion might mean, perhaps helping to define the impact. He also questioned if there were concerns around federal sharing.
    - **Jonathan Coleman** commented that regarding federal sharing, he believed that issue had been resolved.
- **Andy Truscott** asked about policing the attestation between the qualified health information networks (QHINs).
    - **Zoe Barber** answered that the Recognized Coordinating Entity (RCEs) would manage attestation and policing the requirements. She suggested that the TEFCA TF could make a recommendation to add to the Minimum Required Terms and Conditions (MRTC).
- **David McCallie** asked if this would affect the data in summary records exchanged through QHINs. He questioned if there are unintended consequences of CUI that should be considered.
- **John Kansky** noted that what is in TEFCA should not create a barrier. He suggested the following:
    - It needs to be implementable and not create an obstacle or a burden.
    - He suggested that the broader concern is to ensure there are no unintended consequences of creating a two-tier network.
    - He also suggested that this could morph into security tagging, which is a way to deal with CUI.
- **Andy Truscott** suggested deferring this. He suggested that this has been done in other jurisdictions and not too much should be made of this.
- **John Kansky** suggested that the members review the information shared by Jonathan Coleman (link provided in the public chat comments) and discuss once everyone has an opportunity to review.

SECURITY TAGGING

John Kansky transitioned to Security Tagging and noted that ONC is requesting comment on this item.

- **David McCallie** noted his interpretation is that this is suggesting to start with tagging as a policy goal and then figure out what to do later. He noted that if he is interpreting correctly, this path makes sense.
- **David McCallie** also commented that provenance tracking needs to be solved first, before layering on complex behaviors related to security. He noted that there is a need to know where the data is coming from, which impacts what one is allowed to do with the data.
- **Sasha TerMaat** noted that in response to the notice of proposed rulemaking (NPRM), the HITAC suggested forming a task force around data segmentation. She suggested that there should be a similar recommendation here noting that governance work is needed because there isn't the widescale implementation of this type of tagging.
    - **John Kansky** agreed with this recommendation.
- **Sasha TerMaat** commented that with security labeling, there are three areas to think about:
    - How to apply the labels?
    - What to do when receiving something that is labeled?
    - How to handle governance or disputes about labeling?
- **Jonathan Coleman** noted that there are security controls that an organization can implement. This is a subset of NIST 800-53 and was selected to apply to the healthcare environment, but is not specific to tagging. This is not specific to security labeling, but rather security best practices.
- **David McCallie** agreed with Sasha TerMaat's comments. He commented that this needs more study before it is baked into the MRTCs.
- **Andy Truscott** commented that he agreed with both Sasha TerMaat and David McCallie. He commented that this needs to be explored more and that tagging data is hard.
- **Denise Webb** commented on the point about a standard, from her military background, there was security labeling, and there could be lessons learned from the Department of Defense (DoD).
- **Jonathan Coleman** noted there is a standard for data segmentation for privacy, but it is only for Consolidated - Clinical Document Architecture (CCDA).
- **Noam Artz** noted that there have been things done without tagging, instead done as a clinical decision support exercise. He noted that he wasn't sure that the tagging approach will ever work.
    - **David McCallie** commented that the downstream behavior needs tagging or provenance.
- **Andy Truscott** suggested moving on and letting the future task force resolve these issues.

CERTIFICATE AUTHORITY - BACKUP AND RECOVERY

- **David McCallie** commented that he questioned why this belongs at all.
- **John Kansky** suggested a recommendation that this feels like one of several requirements that could be placed on QHINs
    - **David McCallie** commented this is a technical detail that seems to fall under the RCE area of responsibility.
    - **Andy Truscott** and **Denise Webb** suggested focusing on the policy goals to recreate the security environment if there is an event that causes corruption.
    - **John Kansky** suggested an edited recommendation that focuses on the policy goal to create the security environment and leaves the technical detail to the RCE.

IDENTIFICATION PROOFING AND AUTHENTICATION

- **Zoe Barber** noted the original question about this came from Arien Malec who was not able to join. She shared that he was asking how the new versions in National Institute of Standards and Technology (NIST) compare to the requirements in the previous version. She asked Johnathan Coleman to confirm whether these are the latest levels.
    - **Johnathan Coleman** commented that the burden is on the entity issuing the credential.
- **Andy Truscott** commented that in the QHIN agreement with the RCE, there will be a trust arrangement made.
- **Johnathan Coleman** commented that there is wiggle room, as there can be two single-factor authenticators.
- **Andy Truscott** asked if there is a national standard for authentication.
    - **Johnathan Coleman** commented that he was not aware of anything.
- **David McCallie** commented that this is an area where there could be a lot of change over the next few years.
- **John Kansky** summarized that there shouldn't be two standards. The standard suggested is appropriate, but the industry may not be ready yet.
- **Mark Savage** commented that based on past recommendations (e.g., the Health IT Policy Committee's Privacy and Security Tiger Team) this needs to be two-factor authentication or more.
- **Andy Truscott** commented that he was concerned about usability and felt it was necessary to keep decisions local.
- **David McCallie** commented that there is nothing wrong with raising the bar to two-factor authentication, which has become the norm.

ADDITIONAL QUESTIONS

Before closing the meeting, **John Kansky** asked the TEFCA TF members if there were any additional questions.

- **Mark Savage** asked what TEFCA says about application programming interfaces (APIs).
    - **Zoe Barber** commented that there is a distinction between document exchange versus resource-based exchange. She noted that Integrating the Healthcare Enterprise (IHE) profiles are discussed in TEFCA. She commented that there is value in exchanging both documents and resources. The QHIN framework is based on what is out there today and implemented already. Understanding that there is work around fast healthcare interoperability resources (FHIR) APIs, she suggested that ONC did not want to step in the way of that work. The RCEs will determine when that is ready to be implemented as a requirement.
- **Mark Savage** asked if there could be a placeholder to express an expectation for what is to happen.
- **David McCallie** commented that he agreed with what Zoe Barber shared, as it makes sense to start with document-based exchanges.
- **Andy Truscott** commented that there is a need to be thoughtful about how to promote advancement.

Cassandra Hadley opened the lines for public comment.

Public Comment

There were no public comments.

COMMENTS IN THE PUBLIC CHAT FEATURE OF ADOBE

Johnathan Coleman: https://www.archives.gov/cui/registry/category-detail/health-info

Andy Truscott: https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf <-- Marking Handbook

Mark Savage: For future reference, page 18 on screen shows as page 19 on my print version. Just noting to avoid confusion with page numbers across our future discussions. There may be two-page numbers.

Johnathan Coleman: There is a normative HL7 standard describing the labels that can be applied. There is a reduced value set for CCDA (N, R, VR)

Andy Truscott: I was pointing to work from other jurisdictions: e.g. HL7v3 definition by UK for Sealed Envelopes.

Andy Truscott: Certificate Revocation Lists (in case I was muffled)

Julie Maas: The Certificate Authorities would just need to establish their Trusted Agent processes in their CPs to achieve that "chain" effect.

Andy Truscott: Julie: I think all we're trying to say is that CPs must include appropriate procedures for recreation of the Security World in the event Roots are unavailable.

Julie Maas: For TEF actions, is MFA perhaps even greater a concern than whether a user is [authorized to access PHI within an EHR], LoA3, or IAL2?

Johnathan Coleman: NIST Gives examples of the combinations of authenticators allowed at AAL2, section 4.2.1 https://pages.nist.gov/800-63-3/sp800-63b/sec4_aal.html#singlefactorOTP

Next Steps and Adjourn

Zoe Barber noted that the TEFCA TF is working towards sharing draft recommendations at the June 19 HITAC meeting. She also noted that there are notes and transcript posted on the HealthIT.gov website from each meeting.

John Kansky commented that he will work with Arien Malec and Zoe Barber to draft recommendations based on the comments that have been shared.

The meeting was adjourned the meeting at 2:30 p.m. ET