Trusted Exchange Framework and Common Agreement Task Force

Transcript
June 20, 2019
Virtual Meeting

SPEAKERS

Name	Organization	Role
Arien Malec	**Change Healthcare**	**Co-Chair**
John Kansky	**Indiana Health Information Exchange**	**Co-Chair**
Noam Arzt	HLN Consulting, LLC	Public Member
Laura Conn	Centers for Disease Control and Prevention (CDC)	Member
Cynthia A. Fisher	WaterRev, LLC	Member
Anil K. Jain	IBM Watson Health	Member
David McCallie, Jr.	Individual	Public Member
Aaron Miri	The University of Texas at Austin, Dell Medical School and UT Health Austin	Member
Carolyn Petersen	Individual	Member
Steve L. Ready	Norton Healthcare	Member
Mark Roche	Centers for Medicare and Medicaid Services (CMS)	Member
Mark Savage	UCSF Center for Digital Health Innovation	Public Member
Sasha TerMaat	Epic	Member
Grace Terrell	Envision Genomics	Public Member
Andrew Truscott	Accenture	Member
Sheryl Turney	Anthem Blue Cross Blue Shield	Member
Denise Webb	Individual	Member
Lauren Richie	Office of the National Coordinator	Designated Federal Officer
Cassandra Hadley	Office of the National Coordinator	HITAC Back Up/Support
Zoe Barber	Office of the National Coordinator	Staff Lead
Kim Tavernia	Office of the National Coordinator	Back Up/Support
Alex Kontur	Office of the National Coordinator	SME
Morris Landau	Office of the National Coordinator	Back-up/Support

Michael Berry	Office of the National Coordinator	SME
Debbie Bucci	Office of the National Coordinator	SME
Kathryn Marchesini	Office of the National Coordinator	Chief Privacy Officer

Operator
All lines are now bridged.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Thank you. Hello everyone. Welcome to yet another TEFCA Task Force call. A quick roll call of the members. I see here we have John Kansky, Arien Malec, Sheryl Turney, Cynthia Fisher, David McCallie, Noam Arzt, Grace Terrell, and Laura Klein. Are there any other task force members?

Denise Webb – Individual – Co-Chair
Denise Webb is on. I'm still joining you though. Hi.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Hi Denise. Anyone else?

Arien Malec – Change Healthcare – Co-Chair
I see Carolyn Peterson on as well.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
All right. it looks like she'll be joining us soon. Okay, at this point I will turn it over to our Co-Chair to get us started.

Arien Malec – Change Healthcare – Co-Chair
Hello, I'm back. And as Lauren said, the meetings will continue until morale improves. We have a fairly steep process to get through in order to get to final recommendations. We had a good readout of the draft recommendations to the full advisory committee yesterday. We got a lot of really good feedback from that, so I think we are in a good place to finish out our recommendations. But we do have, a fair amount of work between now and then. There are a couple places where we have alternative formulations. We've polled a sense of the task force to get to consensus and which finalize the wording of the recommendations. What we are going to do right now, and apologies for the confusion earlier today, is we are going to go through our approach, I think has been really successful, going breadth first before we go depth first.

So, we have taken a lot of the feedback and refined some of the recommendations, but we'd like to get through the remainder of the first path's recommendations. We sent everyone kind of as a teaser an updated recommendations letter. I think we have more work to do there both in terms of feedback today as well as potentially reordering and renumbering some of the recommendations. But today we're gonna get through Privacy and Security to make sure we've done a good thorough first pass of our recommendations. And then in subsequent meetings, we're gonna go back through the recommendations letter as it's been revised and focus on areas of controversy as well any fine-tuning that needs to happen to make sure that the recommendations reflect the full sense of the task force.

So, I will pause there to make sure this process makes sense to everybody. I assume silence means everybody on board. So, can we put the Privacy and Security draft recommendations up and –

Zoe Barber – Office of the National Coordinator for Health Information Technology– Staff Lead
Arien, you might want to mention...this is Zoe. We apologize, but two documents were sent to you today...two draft transmittal letters were sent to you today and so you will want to look at the one that has the older date on it and under the initials a.m. The previous one we forgot we had made edits to it for the call yesterday, so it doesn't have a summary of disclosures and security parts in it.

Arien Malec – Change Healthcare – Co-Chair
Yes. So, you should get two documents and please look at the older one. We are going through that virtually right now so we will start with 5.2 and then go to Section Six. So, 5.2 discusses the Summary Disclosures and Auditable Events and the general sense of our findings and recommendations here are that auditable events and summaries of disclosure should be aligned. And that the QTF should not dictate the functional requirements that the MRT sees but should describe the functional requirements both for auto-retention and auditable events and make sure that auditable events and the auto-retention period aligns with the summary of disclosure requirements. So, that is what Recommendation 12 outlines.

I will pause to see if there is any...boy this is one of those things where hopefully, Zoe, I don't know if you are seeing the hand raising, but I have expanded the screen share so I can read it. So, it would be useful if someone else could look at hand raising to make sure that we are responsive to anybody who wants to get in.

John Kansky – Indiana Health Information Exchange – Co-Chair
Arien, I can help out there as well. There are currently no raised hands.

Arien Malec – Change Healthcare – Co-Chair
Great. So, I will assume that, given the lack of raised hands there is agreement on this language. The second piece here is recommendations on the summary of disclosures and the sense of the recommendation here is that if you had to do summaries of disclosures across network, and align it altogether with the single point of reporting, there would be a lot of work that would need to happen in order to make that happen. And we wanted to clarify the requirement that the summary of disclosures really is between the organizations as the direct relationship with the requesting individual and any disclosures that have happened with respect to that organization and their selected QHIN.

David McCallie – Individual – Public Member
Arien, it's David. I don't remember the language, but if a person wanted to find out where their information has been shared, is that possible with this requirement?

Arien Malec – Change Healthcare – Co-Chair
I don't believe it's possible with this requirement. I think this requirement would allow me to discover where any organization that I have a direct relationship with would allow me to discover any disclosures that have happened with respect to that relationship. So, including times that my information has been pulled via the QHIN from other members, as well as times where the information from the members has been requested or other QHINs have been requested by my home QHIN. But if there were a hypothetical...if there were another participant or participant number housed in some other QHIN that had pulled data from a third QHIN, that QHIN 'A' wouldn't have the accounting of or summary of disclosures relative to that. Presumably I would have a direct relationship with the organization that was pulling my data, but I do think there are some cases where you need to do a little extra work to find all the places where there has been disclosure.

David McCallie – Individual – Public Member
Well, I wonder if the sense of...if ONC senses that this should be a QHIN burden to basically how aware your information has been sent. I mean I think that's the use that I think most people would identify with is where has my information been shared.

Arien Malec – Change Healthcare – Co-Chair
That's right.

David McCallie – Individual – Public Member
And I don't want to poll every possible healthcare organization to find out if they got it.

Arien Malec – Change Healthcare – Co-Chair
I think that is right. It might be worthwhile rewording Recommendation 13 to say, "That they should require a summary of disclosures from the entity and associated QHIN with the direct relationship" and then maybe parentheses 's' to the requesting individual, including for particular times when the disclosures...when the direct relationship has pulled data as well as disclosures when data has been requested from the direct relationship and associated QHIN.

David McCallie – Individual – Public Member
I think that's right. I would caution of course, that's a capability that goes beyond what current networks do. So, that would be a significant technical lift, but it seems reasonable from a policy goal to move in that direction. You should be able to track the flow of your information through TEFCA as an individual.

Arien Malec – Change Healthcare – Co-Chair
Yes. In Commonwealth for example, we audit all of the information. And so, being able to provide that information is relatively simple. But to my knowledge, I don't know that we have an easy to plug in summary of disclosures form, nor do I know that anyone has requested it

David McCallie – Individual – Public Member
Right. Right. It' s just that by –

Arien Malec – Change Healthcare – Co-Chair
It's useful to have if somebody does.

David McCallie – Individual – Public Member
The data is being captured; it's just not being made available. We should be clear what we think should be available. And I think it's between you and your direct participant and their QHIN, where did their information flow in both directions?

Arien Malec – Change Healthcare – Co-Chair
Correct.

David McCallie – Individual – Public Member
It's a QHIN audit being made available through your direct participant.

Arien Malec – Change Healthcare – Co-Chair
Any other comments on Recommendation 13? Cool. So, I think we've got the... David, I think it's a really useful clarification and I think we've got agreement on Recommendations 12 and 13. So, now we go on to Section 6 and there's a lot of preamble here. So again, just to summarize the discussion we had in this topic, I think we recognize there are multiple cases where there may be systems that span national borders. There are servicemembers and federal employees that may wish to access data in the United States. There are cases where people are traveling and so we don't want to have a blanket prohibition on data traveling outside of the United States. And, we also wanted to note that talking about data at rest and the location of data at rest is important from a privacy law or governing law perspective, but it's only one of the security risks. So, our two recommendations: number one is that ONC should focus on security requirements for the networks such as...I don't know what 'data description arrest'... I'm not sure what that is saying, nor do I understand verifiability of access pathways but –

Sasha TerMaat – Epic – Member
Could that be 'data encryption at rest', Arien?

Arien Malec – Change Healthcare – Co-Chair
'Data encryption at rest' makes sense.

Sasha TerMaat – Epic – Member
I pointed that out because I thought that was a mistake.

John Kansky – Indiana Health Information Exchange – Co-Chair
I suppose that's AXIF as opposed to World War II AXIS.

Arien Malec – Change Healthcare – Co-Chair
Yeah. It's Verifiability of Access Pathways. It's ACCESS, but this probably is one where we need to ...ONC should focus on risk-based requirements for the networks as opposed to all of the detail. Here would be my example and recommendation. So, for Recommendation 14, I would rather say, "ONC should focus on a risk-based set of security requirements for the network...not for the network, but for QHIN's... and not make where the data resides a central criterion for security."

And Recommendation 15 "Is the restriction of the QHIN operation in the United States reasonable?" ONC shouldn't frame restrictions in terms of cloud services. And it's less that cloud service is vague and undefined and more that it inadvertently leaves out a data center operation that I might run that could be based in Mexico or China or someplace like that which is a day cloud service per se. So, it's not just vague and undefined but it's also misleading. So, I would rather say the restriction to have QHIN operations is reasonable. ONC shouldn't frame restrictions in terms of cloud services, but instead the restriction should be limited to data center operations for data at rest.

Sasha TerMaat – Epic – Member
Arien, when you say, 'data at rest', is that about that QHIN data at rest or is this also about the people who access data through a QHIN?

Arien Malec – Change Healthcare – Co-Chair
That's a really good question. I would say it's the QHIN's data at rest. That's a great clarification.

Sasha TerMaat – Epic – Member
I think it would be too difficult and have unintended negative consequences to try to restrict access to data at end points that they are connecting to, but I think it would be helpful to clarify that in the recommendation.

Arien Malec – Change Healthcare – Co-Chair
I completely agree and it's a great point. If there is appropriate regulation for risk-based security. For example, a hospital or healthcare entity where they have their data reside. That may be an important matter, but it's not a TEFCA matter. We really shouldn't be trying to back regulate those kinds of activities through the TEFCA. So, this is really related to the QHINs operations. I completely agree.

David McCallie – Individual – Public Member
Arien? Have we reached an opinion on the broader principle of no EHI used or disclosed outside the U.S.?

Arien Malec – Change Healthcare – Co-Chair
Yes. I think we have, and I think our perspective there is that there are many reasons why EHI should be used or disclosed outside of the United States.

David McCallie – Individual – Public Member
Do we need a recommendation that contradicts that flat-out statement 6.1 that says, "No EHI are used or disclosed outside the U.S."?

Arien Malec – Change Healthcare – Co-Chair
Yes, we should. Great point. We talk about it in the findings, but we don't actually have a formal recommendation.

David McCallie – Individual – Public Member
Yes, exactly.

Arien Malec – Change Healthcare – Co-Chair:
Thank you. Oh man. Good. Okay. So, I think we are done with that section. I'm going to pause a little bit to read ahead to realize I have a difficult topic ahead of me, but I will pause to make sure that 6.1...that we feel like we're in a good place with the recommendations there. All right.

Let's go to 6.2 Controlled Unclassified Information. So, we discussed this and our concern here is that you end up creating a two-tiered network or basically defining additional driving QHIN operations to the level of FISMA, SEDRAMP, DOD-SRG and the other somewhat confusing set of federal information security requirements. So, that is our comment and then I don't know...and I'm not sure... I solicit good opinions on what an appropriate recommendation would be because I think we could recommend that ONC drop the CUI distinction. I actually think that might be a good idea because whether EHI is classified as, for example SRG low, versus medium, versus high. Or the appropriate fed ramp designation of of medium versus high depends on use and context and I think I think we've articulated many examples where it may not be CUI.

So, I would propose just dropping the CUI section. I assume ONC put it in place because there are federal partners who have particular security designations and they want to be able to use the TEFCA

and QHINs to access data. So, I would love to hear a perspective on how to address the potentially conflicting requirements we have here.

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
This is Debbie. I assume you discussed it in detail at the last meeting?

Arien Malec – Change Healthcare – Co-Chair
It was a few meetings ago, but we did have a vigorous discussion of this topic.

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
True, it would be a federal requirement for federal release of data but, as you say, it may not necessarily apply to how it goes downstream. So, to have nationwide exchanges, we do want federal partners including the Mayor so what is the middle ground?

Arien Malec – Change Healthcare – Co-Chair
That is exactly the question and the reason I'm framing the question is I don't know what the middle ground is. Does the CUI designation and fed ramp medium give the majority of federal partners ability to use QHINs? Sorry, this is an area I know too much about, but one of the ironies of this world is that, for example, DOD and VA will put on their own particular security requirements associated with their operations in their facilities. And then their patients will wander outside of the VA hospital or outside of the military treatment facility and then go across the street to a regular commercial hospital and receive care there. So, the DOD classifies DHI as readiness data and as such effectively SRG high and the same day they are sitting across the street in a hospital. And to be honest, who knows what information security requirements are there. So, this topic, I just don't know what the middle ground is that provides maximal exchange, for example, relative to SSA for disability determination or relative to VHA for C Basis services.

John Kansky – Indiana Health Information Exchange – Co-Chair
Arien? David has his hand up.

Arien Malec – Change Healthcare – Co-Chair
Okay. Go, David.

David McCallie – Individual – Public Member
I share your fear about the confusion that this could introduce, but I wonder if it may be a gross oversimplification. Wouldn't it basically boil down to those entities that have restricted data to put the burden on them to just not share it across the network if they feel it's not shareable, rather than to put their rules across the entire network? In other words, if you can't share data that you feel is relevant to readiness, then don't share it. The rest of the network doesn't need to know what the rules are because it's not relevant to them.

Arien Malec – Change Healthcare – Co-Chair
That's the justification for basically kicking this section and that was exactly the thought process that I had. Let's kick this section, and recommend taking this section and basically say a federal partner...we may want to have a federal QHIN that holds to whatever common denominator security requirements that the participating organizations, agencies and departments want to have on it and they can spend all the money and security that they want to. And then, it would be their choice whether to disclose data and it would be their choice relative to whether to request data.

David McCallie – Individual – Public Member
Yes. So, disclose conservatively, consume liberally.

Arien Malec – Change Healthcare – Co-Chair
And basically, put the onus on them and whether they contract with to put those requirements on them.

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
Does that lead to an unbalanced situation where certain participants would be consuming data and never responding because of their security requirements? In general, accepting the fact that I understand there are specific federal requirements, in general it would seem undesirable to have certain participants say, "Our security is higher so we will take all of your data, but we aren't gonna share because you haven't met our security requirements." That seems like a nonreciprocal undesirable situation for the network as a whole.

David McCallie – Individual – Public Member
I think that's true and I think it's a risk. But the other side of it though is if you have higher requirements than everyone else has and you demand that everyone else meet your requirements, don't you put a new kind of burden on that work?

Arien Malec – Change Healthcare – Co-Chair
To be honest, my biggest concern is actually worse than that which is that we get on this process of controlled unclassified data protection and then DOD and VA say, "Sorry I can't use it because we treat DHI differently." And I know the DOD treats EHI differently

David McCallie – Individual – Public Member
What if we specifically recast this around controlled unclassified information as opposed to general lack of reciprocity that Sasha was concerned about and just say specifically with respect to CUI, the burden should be placed on the organizations that must abide by the rules to disclose appropriately?

Arien Malec – Change Healthcare – Co-Chair
In other words, a limit to protect and disclose appropriately?

David McCallie – Individual – Public Member
Yes, but limit it to CUI because that has a definition.

John Kansky – Indiana Health Information Exchange – Co-Chair
Arien, you have Denise and then Deb.

Arien Malec – Change Healthcare – Co-Chair
Okay. Denise?

Denise Webb – Individual – Co-Chair
Okay. So, having come from the DOD, I know that the DOD and federal agencies are really strict about their operations and who they contract with to store data and so forth. But, I'm wondering, because I don't know if we've done deep dives on CUI, but I'm wondering if CUI is what we used to call 'For Official Use Only' which is unclassified information. I did just Google this and CUI does replace the

category of 'For Official Use Only' or 'Sensitive but Unclassified'. You know, it seems to me that our floor on security would encompass the requirements because this is unclassified information. And I'm having a hard time seeing that this will raise our ceiling on security across the network, above what we would have to have to protect EHI anyway. Anyway, those are my comments.

Arien Malec – Change Healthcare – Co-Chair
Okay. Thank you. I definitely appreciate that, who is next?

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
It was Debbie, I think.

Arien Malec – Change Healthcare – Co-Chair
Debbie. Okay.

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
So, the federal agencies may be required to label data on outbound and certainly, federal agencies would accept data that's not...that is their burden agreed to be able to label the data. And I do believe the way the QHIN is now, it's that the QHIN should be able to accept that data and there's no flow down to your participants. So, the burden is on agencies to... I do not believe there is a reciprocal burden for a nonfederal entity for data that's not created in the federal environment to tag that data and send it back to the federal agency.

Arien Malec – Change Healthcare – Co-Chair
Okay. So, I think I hear consensus and I think there's an important caveat in Sasha's comments. I think we are hearing consensus that the burden of CUI and other security designations for EHI should rest on the federal agencies that have those requirements. And then I think there's a second recommendation that says, "Notwithstanding the different security requirements that federal agencies may or may not have, the presence of that additional burden should not lead federal agencies to nonreciprocal exchange whereby they request but never share data. Then, there's a whole lot of how. That's kind of the what.

John Kansky – Indiana Health Information Exchange – Co-Chair
Other than as required by you know, their rules.

Arien Malec – Change Healthcare – Co-Chair
Sure. Yes. That's the tricky bit, right? Is other than is required by their rules, but if it truly is...Andy Truscott was providing the non-hypothetical example of a special forces operator whose data, relative to exposure had implied certain kinds of operations. So, there may be good reasons not to share, but we don't want to be in a situation where just because I have different security requirements I only query and I never share. That's the key part of the recommendation that we want to frame up.

John Kansky – Indiana Health Information Exchange – Co-Chair
Agreed, but they have specific rules to determine what that is and that wouldn't be allowed because they have specific rules. We're not granting a carte blanche notion that you could just up and decide I don't want to share this.

Arien Malec – Change Healthcare – Co-Chair
Well, that's right. But I also shouldn't be in a position just because I have different security requirements that I've got to maintain... internally that I never share information. It should be on a specific case basis.

John Kansky – Indiana Health Information Exchange – Co-Chair
Sure. Where they could find CUI.

Arien Malec – Change Healthcare – Co-Chair
So, I think we have a sense of recommendation. I'm gonna pause there. We're obviously gonna write it up and then review it. I'm gonna pause there and see if that meets people's expectations. Okay. Cool. Now we go on...sorry, I just have to re-enter my security requirements and re-log into my computer. Okay. Security tagging... I think we need to re-write this recommendation, but basically our general concern with security tagging for information in the TEFCA is that this is one of those areas where there's a standard but no policy, and we don't understand the policy requirements.

So, the previous version of this recommendation talked about standards and standards uncertainty. And this is actually an area where we have appropriate standards, we just don't know what to do with the standard when we get it. And so, I think we need to redraft this recommendation a little bit. The general recommendation is, this really should be a CURES and PRN set of requirements. We're supportive of the direction, but we believe until there's actionable policy, it would be inappropriate to put a tagging burden on QHINs and TEFCA. I will pause there.

John Kansky – Indiana Health Information Exchange – Co-Chair
Arien? Would it make sense to tie it to U.S. CDI and basically keep in sync with advances in U.S. CDI?

Arien Malec – Change Healthcare – Co-Chair
Yes, so that's what I meant by the CURES rule that basically, U.S. CDI and other general owned certification rules.

John Kansky – Indiana Health Information Exchange – Co-Chair
Arien, you have Noam and then Sasha.

Arien Malec – Change Healthcare – Co-Chair
Okay. Hey, Noam.

Noam Arzt – HLN Consulting, LLC – Public Member
Hi. Just really quick, just to reinforce this, it's not just that we don't know what to do with it. No one else knows what to do with that either. It's not like this is in use really, even when the standard is defined.

Arien Malec – Change Healthcare – Co-Chair
Exactly. It's a bizarre area where we've got a standard. It says how to tag things, but I keep asking really basic questions like for SAMSHA for example, if I get data and it's tagged and I get data from somebody else and it's not tagged, can I share it or can I not share it?

Noam Arzt – HLN Consulting, LLC – Public Member
Right.

Arien Malec – Change Healthcare – Co-Chair
And nobody can say one way or the other.

John Kansky – Indiana Health Information Exchange – Co-Chair
Well, they'll tell you that it depends on the order in which you got the data which is bizarre.

Noam Arzt – HLN Consulting, LLC – Public Member
But it's even worse than that. The very fact that you're getting tagged in the information, what does that mean? If you look at it, you're supposed to un-look at it?

Arien Malec – Change Healthcare – Co-Chair
Yes. Exactly.

Noam Arzt – HLN Consulting, LLC – Public Member
The whole premise of this to me is a bit absurd.

Arien Malec – Change Healthcare – Co-Chair
That's right. Sasha?

Sasha TerMaat – Epic – Member
One other thought that we discussed previously, the information blocking discussion had recommended us a different task force. And the TEFCA draft actually asked questions about a lighter weight version of use of the standard based on specific value sets. It seems like we could recommend that the task force that we already recommend be created. In particular, consider the scope of what the TEFCA proposes whether this would be worth a starting point and how that would factor into the overall policy recommendations.

Arien Malec – Change Healthcare – Co-Chair
I agree and I think that's just another way of saying that our general recommendation is that that there should be a single line set of recommendations, that the horse here is the U.S. CDI and certification. This is the cart and there is an urgency around policy clarification that the advisory committee has already made recommendations on.

Sasha TerMaat – Epic – Member
Sounds good.

Arien Malec – Change Healthcare – Co-Chair
Cool. Anymore comments here? Certificate of Authority Backup and Recovery...we recommended that this provision be deleted, and I think our recommendation right here is a little bit misleading and mis-worded so I think our recommendation should be that we recommend deleting this provision.

John Kansky – Indiana Health Information Exchange – Co-Chair
Arien, is there any reason to think that the security requirements for QHIN should be any different than the HIPAA security requirements? Have we had that broad notion, or could you keep them in sync at that level?

Arien Malec – Change Healthcare – Co-Chair
We have and we generally made recommendations in areas where HIPPA and MRTCs are defined that if we've got organizations that have dual obligations, that the HIPPA obligation should be primary.

John Kansky – Indiana Health Information Exchange – Co-Chair
It's a basic general thought that they should be the same.

Arien Malec – Change Healthcare – Co-Chair
Yes. So, we've already made comments relative to aligning HIPPA and MRTCs relative to if you are already a covered entity or a business associate for a covered entity. Then your requirements there should generally address all of the requirements you have under TEFCA. And in particular, if there are any specific requirements are extra to the HIPAA privacy and security, that ONC should call those specific ones out and otherwise allow organizations to map their existing HIPPA obligations and VA terms to the MRTCs. I think we already covered all that stuff.

John Kansky – Indiana Health Information Exchange – Co-Chair
So that might be a reason to dismiss this one if it's covered elsewhere.

Arien Malec – Change Healthcare – Co-Chair
Yes. That's right.

John Kansky – Indiana Health Information Exchange – Co-Chair
It would fall under the purview of the other –

Arien Malec – Change Healthcare – Co-Chair
This one is just... I know what's required to be a CA and it's a lot and we should just not...it's just inappropriate to try to define it at this level. we could eliminate this one.

David McCallie – Individual – Public Member
Arien, not to make this harder because I'm not trying to, but what I remember is sort of a version of what you just said now, is that, why would we callout this specific thing if your certificate authority you have other things to do to be appropriately secure .

Arien Malec – Change Healthcare – Co-Chair
Exactly.

David McCallie – Individual – Public Member
So, we should explain that we could recommend deleting this on the basis not that it should not be done, but on the basis that it shouldn't be specified here, it should be part of a broader security program.

Arien Malec – Change Healthcare – Co-Chair
That's right. and it's specific to CA's.

David McCallie – Individual – Public Member
I was getting confused. I forgot that this was specific about the CA aspect which isn't covered under HIPPA, so my apologies for bringing HIPPA up. I wasn't connecting the dots.

Arien Malec – Change Healthcare – Co-Chair
No problem. Okay. So, I think we've got agreement here. I'm gonna pause there to see if we have any other comments or disagreement that we have agreement, etc. Okay. And let's go on to the next section, Identity Proofing and Authorization. So, we discussed proposed levels for identity proofing and authentication and the MRTCs. We think they are reasonable but maybe the industry is not ready yet. Do we have a recommendation here? Or is our recommendation that we are good?

John Kansky – Indiana Health Information Exchange – Co-Chair
I don't know the answer to the question and there are no hands raised, but I will try to throw out what I remember. This is a section that requires...oh, it says identity proofing...so this is IAL2 and it implies... that we are talking about identity proofing not authorization. I'm trying to catch up with where you are. There is IAL2 which is specified for identity proofing and AAL2 that is specified for user authentication. I don't know that we had a whole bunch of discussion about whether either of those are doable. What I recall is that IAL...AAL2 for authentication implied two factor and there was some conversation about pretty much everything we do on the web. People are getting used to doing two factor, so it doesn't seem unreasonable etc. And now we have Debbie and then David.

Arien Malec – Change Healthcare – Co-Chair
Debbie?

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
I was just kind of...what he was saying is basically you are mixing identity proofing and authentication and it's two separate things. So, the requiring two factor for authentication is different than the requirements for identity proofing. So, you just might want to... okay, there you go. Thank you.

Arien Malec – Change Healthcare – Co-Chair
Thank you. David?

David McCallie – Individual – Public Member
I'm generally in favor, because of the power of the TEFCA, to set a pretty high bar there for both proofing of users and authentication of users. However, the place where we might run into conflict is the overarching goal that we want that to be minimally disruptive to existing networks. I don't know enough about what the existing networks require to know if these requirements would be in a serious enough escalation to break them. So, that might be a concern to sort of suggest a staged approach, that sets a target and a timetable to get to this higher level but tolerate a ramp-up if it's disruptive to existing networks.

Arien Malec – Change Healthcare – Co-Chair
That doesn't sound unreasonable.

David McCallie – Individual – Public Member
One of the things we talked about last time, and again I don't think there was recommendation in there, but we discussed and agreed that it would be necessary that participants could accept the identity proofing of participant members and QHINs could accept the identity proofing of participants etc. etc.

Arien Malec – Change Healthcare – Co-Chair
That also makes sense.

David McCallie – Individual – Public Member
It makes sense. I don't know if we need to say anything about it. I'm just throwing it out there. I think it cold be unclear and that's important.

Arien Malec – Change Healthcare – Co-Chair
I think it's a reasonable recommendation that we are not putting...that identity assurance and authentication is one of the activities that can be pushed by a QHIN on to participants and organizations...the flow down terms as opposed to, you have a credentialed physician who can login to their EHR but then they have to do extra work or duplicative work to enable TEFCA. That sounds like a bad idea.

David McCallie – Individual – Public Member
Okay.

Arien Malec – Change Healthcare – Co-Chair
Okay. So, let me reframe the recommendations. So, it sounds like we agree with the proposed ONC MRTCs. We recommend an appropriate time for organizations to harmonize existing identity and authorization practices with the MRTCs. And, we recommend that ONC and the RCE's via the MRTCs allow this identity assurance and authentication to be appropriately delegated via flow down terms and others to participants and participant members.

David McCallie – Individual – Public Member
It's not so much delegated to as fulfillable by.

Arien Malec – Change Healthcare – Co-Chair
Okay.

David McCallie – Individual – Public Member
I'm not sure of the right words, but you see what I'm saying? We're not saying you have to worry about it but, the thought was that if you've already met these with your local systems you don't need to meet them again just to connect to the QHIN.

Arien Malec – Change Healthcare – Co-Chair
I think we are saying the same thing.

David McCallie – Individual – Public Member 00:47:01
We are. The words might be important. I would almost go to acknowledging that the only practical approach to identity proofing is that it lives at the most proximate level to the patient and providers. It's the edge.

Arien Malec – Change Healthcare – Co-Chair
Okay. We will work on the wordsmithing and make another pass at the words to make sure they reflect the sense of the task force.

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
This is Debbie. The reuse of identity proofing is implied already in the TESCA around the indices and events, so maybe some clarification about leveraging what has already been done, but just know that the principal is already there.

Arien Malec – Change Healthcare – Co-Chair
Okay. Thank you. All right. So, we got through a good chunk, all of the outstanding recommendations. At this point, do we want to start the second pass through the recommendations? There are two sensible approaches that we can do. One is to start the second pass through the recommendations. The other is to go to public comment, give everybody a little break in their day, and then we can use the time to format and formulate a revised set of recommendations that have consistent numbering, consistent wording, and are reflective also of the comments of the committee. The more that I say the latter one, the more I like it.

Denise Webb – Individual – Co-Chair
I agree.

Sheryl Turney – Anthem Blue Cross Blue Shield – Member
I agree.

Debbie Bucci – Office of the National Coordinator for Health Information Technology – SME
I will vote for that one.

Arien Malec – Change Healthcare – Co-Chair
So, I think that we have agreed on that course of action and at this point, are there any additional comments before we go to public comment?

Noam Arzt – HLN Consulting, LLC – Public Member
I do have a lingering comment in there that the...see at the bottom of the screen? I was not on the call that generated the agenda that we have been following, but for whatever reason, patient matching didn't make it onto the schedule here. Is there anything we want to say about patient matching given how generally pitiful the strategies still are?

Arien Malec – Change Healthcare – Co-Chair
It's a great comment. The way that we have addressed that is to note that we are really looking for better clarity on the functional requirements for the QHINs. Part of the functional requirements is that, when a request is received of a QHIN, the QHIN has a responsibility to find the appropriate data among the participant and participant members that the QHIN serves and that statement implies but does not require a record locator service, or patient matching and linking, or other kinds of capabilities. I tend to believe, but I'm open to alternatives, but that level of functional requirement is appropriate. And if we get down into the nitty-gritty of patient matching and requirements there, we are really back into the model of defining the technical requirements for the QHIN. But, if you have an alternative approach to this topic or alternative set of recommendations that we want to consider, I think we would all be open for that. Any other comments that folks have on this topic?

Noam Arzt – HLN Consulting, LLC – Public Member
Hi guys. I guess, as long as the other comments make some explicit reference to the patient matching problem I am satisfied.

Arien Malec – Change Healthcare – Co-Chair
Okay. We will make sure we get the next draft in and make explicit recommendations. I think I've lulled everybody into already factoring in extra time in their workday. So, I have engineered a situation where no one wants to raise their voice. Okay. Hearing no other comment, maybe we can go to public comment.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Sure thing. Operator, can we open the line?

Operator
Certainly, if you would like to make a public comment please press *1 and a confirmation tone will indicate you are in the queue. To remove your comment press *2. For participants using speaker equipment, it may be necessary to pick up your handset before using the * key.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Thank you. And I know that Sasha and Caroline joined a little late. Did any other members join after the roll call? Okay. Operator, do we have any comments?

Operator
Not at this time.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Okay. Arien, back to you.

Arien Malec – Change Healthcare – Co-Chair
Great. Okay, John, any closing comments?

John Kansky – Indiana Health Information Exchange – Co-Chair
Nothing from me, thanks.

Arien Malec – Change Healthcare – Co-Chair
I think we have made really good work of the set of recommendations. We're gonna do a turn and come back out with the near final set of recommendations. Just a warning for people that are following on with the recommendation numbering, I think we're gonna end up reordering the recommendation numbers and so it should be a fairly extensive next set of edits. But hopefully the edits will account for all of the comments of the task force as well as the comments of the advisory committee and should be close to final. And then we'll go through a couple more passes of the language to make sure that we've got a finalizable set of recommendations that will serve as the basis for getting approval from the advisory committee. With that I return some time to everyone today

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Thank you, everyone.

Multiple Voices
Thank you. Goodbye.