Health Information Technology Advisory Committee
Office of the National Coordinator for Health Information Technology

Trusted Exchange Framework and Common Agreement Task Force

Transcript
June 4, 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
Johnathan Coleman	Security Risk Solutions	Security SME

Operator
All lines are now bridged.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Hi, everyone, welcome to the TEFCA task force here. The numbers we have John Kansky, Carolyn Peterson, Sheryl Turney, Sasha TerMaat, Anil Jain, Andrew Truscott, David McCallie, Mark Savage, and Laura Khan. Are there any other members that joined that I didn't call? I think we would just pick up on our session around security provisions, but I'll turn it over to John for any opening remarks.

John Kansky – Indiana Health Information Exchange – Co-Chair
Just to frame for the group that we are picking up and working on the matrix where we left off. But I think first Zoe has an introduction to make. Zoe?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes, hi, everyone. So, I just want to briefly introduce Jonathan Coleman, who is going to be joining us today on the call. Jonathan is a principal at Security Risk Solutions, and he consults for ONC around security. So, he will be on the call today to answer any socked-based questions that we have. And Jonathan, if you could just say hey so people could hear your voice.

Johnathan Coleman – Security Risk Solutions – Security SME
Good afternoon, everybody. Thank you, Zoe, it's a pleasure to be here.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you for participating. So, with that, as displayed on the screen, we left off yesterday with CUI or controlled unclassified information. And then the hope for the day is to finish out the remaining discussion items on the rest of the matrix, which if you're counting, is one, two, three, four, five, six, seven, although some of those kinds of covered yesterday. They do all loosely have to do or not so loosely, have to do with security. So, appreciate Jonathan's being here as a resource.

With that, the CUI or the unclassified control information is discussed in 2.1, 6.2.1. I think there were some questions about – I know dealing with CUI is a factor of great interest in dealing with federal agencies. And whether the suggestion in the draft test two are consistent with what the federal agency would require. And that's the second bullet is requirement sufficient to allow federal agencies to participate? And we would certainly want that to be the case. And if there are any questions among the task force, for folks that are unfamiliar with the controlled unclassified information, what that is and why it represents – why it's singled out.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Sorry, John –

David McCallie, Jr. – Individual – Public Member
Go ahead.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
No, go ahead, David.

David McCallie, Jr. – Individual – Public Member

I was just going to ask Jonathan if he had a good summary of what CUI inclusion in this might mean, different from what it was like in the past. Just to kind of update us on what's the impact of this? And then, a second question, more practical maybe, is whether or not there are other issues we ought to be worried about for participating, for example, of VA and DOD around something like certificate policy and the ability to participate in networks that involve non-federal partners. That was an issue in the past. I'm not sure if maybe it's been resolved. But I know in the early days of direct it was difficult to get an on our certificate policy to allow HIS to connect both inside and outside federal agencies.

Johnathan Coleman – Security Risk Solutions – Security SME
Yes, thank you very much. On the latter point, I believe that was resolved, but I don't have that information at hand. We can certainly research that and get back to you. If that's helpful. But I do recall federal health architecture workgroup discussing it and including that is one of the topics in their risk assessment.

Regarding the controls of classified information, so the executive order which requires the appropriate safeguarding of controlled unclassified information. And to the point in hand about is this a requirement and test sufficient to allow federal agencies to participate? I think from a QHIN to QHIN perspective, If the QHINs are going to be safeguarding the information to the same standards for federal agencies require the contractors, then actually should be sufficient. And I believe that that requirement is NIST 800-1721, which is the controls set, which would be used for safeguarding controlling and classified information.

I don't want to speak on behalf of the agencies. I'll think they'll have to make that determination. But at least as far as the QHIN to QHIN exchanges goes, I do believe that this should be consistent with the existing requirements.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, this is John, and not to oversimplify this one, but perhaps to try and – oh, we already have – Andy's got his hand up, so I'm shut up and let Andy talk.

Andy Truscott – Accenture – Member
No, you carry on, John. But just very quickly. Who would be policing that association between the QHINs?

Johnathan Coleman – Security Risk Solutions – Security SME
So, I don't know the answer to that. So, I will have to defer to Zoe on that one. I don't know if it's a self-abscessation or any other kind of policing. But I think it would be consistent with how another type of policing is done, in terms of assentation.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Right, the RCE would manage any kinds of attestation and policing of those requirements.

Andy Truscott – Accenture – Member
I get that, but who would – so, be a self-assentation, and then the RCE would collate that assentation's to say these QHINs are performing appropriately and adequately.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead

Right. So, we don't get into that level of specificity in the MRTCs, that would likely be something that the RCE would add to the ARTCs. And we can, if we want to make a recommendation for the RCE to put something in like that, in the ARTCs, that would be great.

Johnathan Coleman – Security Risk Solutions – Security SME
Yes. I think that would be excellent.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay so and this is -- go ahead.

David McCallie, Jr. – Individual – Public Member
So, it's David. If you don't have questions from other people, I can give us more to talk about. I don’t know, are we using the HIN… Okay, well if not, again back to sort of what this truly means. And I am concerned for example, would it affect the data that's included in summary records that are exchanged through QHINs, even if the patient or citizen was not in active service or being solicited by federal agencies. So, could you end up with sort of a strange situation that you have to form your PDA summary record differently if the request is coming from or going to a federal agent? I guess I'm really asking if we have an idea about the unintended consequences of CUI, or maybe they're intended consequences, but not yet explored consequences of adding the CUI requirements, which I don't have a good sense of what they actually mean.

John Kansky – Indiana Health Information Exchange – Co-Chair
I don't want to imply I have any experience or more knowledge than I have in this area. I think unexplored may, and I'm openly appealing to any of the phones that want to comment, but I believe this is a new executive order. It’s causing organizations, in my frame of reference, is working with the eHealth exchange. And saying okay the federal government has new requirements related to handling CUI. They are holding out NIST 801 71 as the standard. And there's a little bit of scrambling. This is the first word that came to mind, to try and say, okay, is that reasonable? can we make the federal agencies comfortable and happy with the compliance with their expectations, and at the same time have it be implemented in a way that doesn't make things overly difficult. I don't know that the question is answered or people on the phone have an opinion. So, there you have it.

Andy Truscott – Accenture – Member
No, no, no. I’m pausing and thinking, John.

John Kansky – Indiana Health Information Exchange – Co-Chair
I will pause longer.

Johnathan Coleman – Security Risk Solutions – Security SME
This is Johnathan. If it’s helpful, I put in the chat, the link to the definition of the CUI category of health information as posted by national archives.

John Kansky – Indiana Health Information Exchange – Co-Chair
Yes. I’m looking at it. I don’t know that I’m going to be able to take this in a comment on it intelligently on the fly.

David McCallie, Jr. – Individual – Public Member
Yes. I looked at it before and couldn’t figure it out.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, David is your concern that – I'm going to start wordsmithing a little bit in my brain. Given that this is unexplored, we want to make sure that whatever is in TEFCA, one, is consistent with what the federal agencies are requiring so that we don't create a barrier to the sharing of information. Two that it's implementable in a way that doesn't create an obstacle or burden that think you were alluding to. We don't really know what that recommendation means, but it wouldn't hurt to say something like that. Is that a fair statement?

David McCallie, Jr. – Individual – Public Member
Yes. The broader concern, and again it's based a little bit on the experience in the early days of direct, was that in effect, the differing requirements created a two-tier network, which defeats the purpose of having a bridging network if there are two tiers. So, the goal would be, I guess in my mind's eye, to make sure that these requirements don't have the unintended side effect of creating a two-tier network. You're either talking to a federal partner, or you are not. And having to do everything differently if you are or aren't talking to a federal partner. So just walking through the details to make sure that doesn't happen what I guess be my recommendation. And that's all I know right now. I wish I could be more specific.

John Kansky – Indiana Health Information Exchange – Co-Chair
And I will make the comment that this may be going to morph into the discussion of the next, and I don't want to admit my degree of ignorance going into that, is security tagging, I know it's potentially a way of dealing with CUI, and our next topic to deal with in TEFCA. But I see that Andy has his hand up. Andy?

Andy Truscott – Accenture – Member
Yes, hi, John. I was just going to suggest that maybe we defer this for the time being and give us all a job to explore both the link that Jonathan posted and the child link to that that I posted, that's the actual handbook. Honestly, I'm inclined not to make too much of a big thing of this. It just document marking. And It's pretty explanatory and pretty well defined. And it has been done in other jurisdictions before.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. So, thank you, whoever, excel, or whoever captured the recommendation. And that will guarantee that we poke the group for further discussion we get the draft recommendations. As Andy suggested, encourage those folks to read up a little bit and think, in case that comes up with a – unless it's a deeper comment.

With that, I'm going to transition to security tagging. And I think I was the one who offered the example of CUI only because that's the time I heard it associated, but I don't want to imply that I know more than I do. So, referencing where this appears in TEFCA. It's in the, I don't know what you call that section, is not exactly preamble. But it was in, my copy, it's on – security labeling on Pages 19 and 20. And I believe it's just a request of – ONC is requesting comment if I recall. Does anyone from ONC, oh wait, we have hands up. David, you are in the queue, followed by Sasha.

David McCallie, Jr. – Individual – Public Member
Yes. So, the way I read the language, and I will admit I read it a while ago and haven't reread it based on our recent conversation. So, I may be slightly out of sync here. But is that it was tagging of sensitive materials, but not a whole lot of other requirements on what those tags would cause to happen

downstream. And if that's the way it was structured, I think that makes good sense to defer the complexity of how to handle the security tags to actual implementation choices based on the RCE and interaction with the stakeholders, in the context of a very difficult technical problem and sort of rapidly evolving standards that need to be fleshed out before they are forced on everybody.

If that's a spirit of it here to start with tagging and then figure out what to do about that later, then I think that makes sense. I would restate though that the broadscale experiments on detailed complex handling of downstream structured tag data are an unexplored space. The little bit of work that has been done has not been done in scale. So, I think it would be very wise not to over complicate the technical spec at this point and just state that it's a policy goal that. That it be supported incrementally in the future as standards evolve and permitted. But maybe I misread that. Yeah, go ahead.

John Kansky – Indiana Health Information Exchange – Co-Chair
Reading from the draft, too – I'm pulling a couple things out of context. ONC is considering the inclusion of a new requirement regarding security labeling. And therefore we, meaning ONC, have limited proposed requirements to four of the most commonly required sensitive categories. And ONC is requesting public comment. There was also a statement earlier in the paragraph that said. Currently, security labels can be placed on data to enable an entity to perform access control, blah, blah, blah. I had no, personally no experience with what current security labeling industry experience is, and it sounds like, David, you were referring to that.

David McCallie, Jr. – Individual – Public Member
Yes. And I'll add one…

Sasha TerMaat – Epic – Member
John, what page was that?

John Kansky – Indiana Health Information Exchange – Co-Chair
Sorry?

Sasha TerMaat – Epic – Member
John, what page was that?

John Kansky – Indiana Health Information Exchange – Co-Chair
In my copy, it is 19, but I think I have an earlier version. It might be 20 on all the others.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
No, it's Page 18, and it's also up on the screen if people can see it.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you.

David McCallie, Jr. – Individual – Public Member
One additional comment, if I can piggyback on the end of mine before we go further. It always struck me that you need to have the provenance tracking first before you attempt layering on complex behaviors that are related to the security. We need to know where the data is coming from. Because that will affect what you are allowed to do with the data. So, I am a little surprised that provenance

doesn't take a prior role here, get a higher priority, and then add security tagging in the context of provenance. Because those two go hand in glove in my mind. But I will stop there.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you, and Sasha has been waiting patiently. Sasha?

Sasha TerMaat – Epic – Member
Oh yes. So, I was thinking about the discussion of security labeling, and also some of the conversation we had in the committee about the proposed data segmentation standards concerning the other rule. And I think some of the same concerns with the committee articulated about standards in that proposal would still be true, right? There's a lot of technical work to be done to implement them. There's a lot of governance work that would have to be clarified to move the industry forward. Kind of like David said, there are not widescale implementations of this type of tagging what the implications are. And some of that has to figure still out. Overall, I thought that the scope prioritization that ONC proposes here, to say what if we pick this specific value set and label documents that contain something within that value set. In my mind, it is a much more practical place to start then the broad scope of the standard as proposed in certification. But so, I think this is, the thinking here I think it's a good direction.

However, since the committee proposed that there be a task force that looked into the implementation of data segmentation in general, that was one of the regulations with respect to the other rule, it seems to me that we should refer to the same recommendation here. And to say that we recognized previously that there could be value to this work, but there's a lot of complexity there. And that perhaps that workgroup that we recommended be formed in the other recommendation, would evaluate the thinking ONC has here as a possible starting place as they would do the analysis.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you, that made great sense. So if you repeat, and it looks like it's getting captured, is that while the recommendation in TEF-2 is, in your view, reasonable, that we want to call out that the, I think it was information blocking task force, has recommended separate groups that look into data segmentation. And that we want those to be consistent, and perhaps recommend that workgroup take a look at what's in TEF-2.

Sasha TerMaat – Epic – Member
Yes. And just to maybe qualify my assessment slightly that this was reasonable. With security labeling, I think there are two or three different areas to have to be thought about. One is how do you apply the labels. One is what you do when you receive something that is labeled. And the third is, how do we handle governance are disputes about labeling.

And so, the proposal that ONC has made here addresses the first one. It would be easier to apply labels if we can do pragmatically by saying oh anything with a particular code in this value set should be labeled in a particular way. And that resolves a lot of like the workflow concerns about the burden of labeling and so forth.

However, this doesn't, and I think David was saying appropriately, although I think someone has to make a decision about it, doesn't say what you do when you receive something that's labeled. And nor does it sort of clarify how the RCE or other entities would govern any sort of disputes about, hey, you sent me something that is labeled, but I don't know that label means. Now, what happens? And so, I do think it is still significant for the work that would have to be done. Even though this is a practical way to address a portion of the challenges, it doesn't make the whole implementation I guess ready to go, if that makes sense.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. This might be – inviting Jonathan to comment. Is 801 71, does it speak to security labeling as part of CUI and I know kind of mushing two things together. Or is 801 71, is it silent on security tagging?

Johnathan Coleman – Security Risk Solutions – Security SME
Yes. So essentially, so for the most part, it's silent on security tagging. What 171 is a list of security controls that an organization can implement to help protect the computing environment with which the health information is flowing. So, it's actually a subset of nest 853, which is what the federal agencies currently use for their authorization processes. And the subset of controls has been selected as a tailored set by NIST to deemed applicable to the healthcare environment. So, it's not specific to tagging. It contains several different security controls. And they vary, and they include things like including a warning banner or a login banner, those kinds of things. So, it's not specific to security labeling.

John Kansky – Indiana Health Information Exchange – Co-Chair
Got it, so it's much more general to security best practices.

Johnathan Coleman – Security Risk Solutions – Security SME
That's correct.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. David and then Andy. You guys are my best customers.

David McCallie, Jr. – Individual – Public Member
I'm trying to remember what I raised my hand about. I think I want to just agree with everything Sasha said. I think this stuff is far more complicated than it appears on the surface. One thing is if you have labeling but no actions required, you are kind of marking the records and saying here is the juicy stuff. Because you're identifying the things that somebody thought were especially sensitive, but you don't have any policy rules on what that means in terms of how you treat the data downstream. Which might have a completely unintended consequence from someone concerned about privacy.

So, I think it needs a lot more study before it's baked into the MRCs or MRTCs, whatever we call these things. Let the workgroups figured it out, and then the RCE work with stakeholders to gradually move us forward.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. And I see that we captured Sasha's list of 1,2,3 things which I thought was a good framing. So, thanks to both of you. Andy.

Andy Truscott – Accenture – Member
So, just to part on with Sasha appreciation society then, yes, I agree. And David actually as well.

John Kansky – Indiana Health Information Exchange – Co-Chair

I agree with you, Andy.

Andy Truscott – Accenture – Member
Well, obviously. I do think this is an area that has to be explored **[inaudible] [00:26:21]** I think we are getting to it here **[inaudible]** increasing level of concern over we'll update, what are the what if scenarios where we might not want to share all information, and how can a **[inaudible],** or a provider best control that. You know, Sasha and David both talked about tagging data is very hard. And expecting the standards would make that much magically happen without further work, it's definitely needed, I think in my opinion. The HITAC suggest to ONC a task force be created to enable that to be looked at further. And I think we absolutely need to look at that. I would be tempted to allow TEFCA to carry on it and have the placeholder for this as it comes across and gets defined better. John that would be my suggestion at this point.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. And you guys can laugh at this, it's funny, but is there a national standard, nationally accepted standard for security tagging or that why we're talking about this as largely unexplored because is no such thing?

David McCallie, Jr. – Individual – Public Member
There is no such thing.

Andy Truscott – Accenture – Member
No, there's no such thing. There is **[inaudible]** is available for it in some of the messages at the time. I think, **[inaudible]** inside of the U.K. went through his and sort of the whole **[inaudible]**.

John Kansky – Indiana Health Information Exchange – Co-Chair
Hey, Andy, we are getting about two out of three words. If there's any way to improve that.

Andy Truscott – Accenture – Member
Are they good words?

John Kansky – Indiana Health Information Exchange – Co-Chair
The ones I heard were fine, yes.

Andy Truscott – Accenture – Member
So just opportunistic have gone through this. HL-7 B-3 messages have been defined, for example, by the **[inaudible]**. But that work would need **[inaudible]**.

John Kansky – Indiana Health Information Exchange – Co-Chair
There goes, Andy. Andy, if you can hear us, we can't hear you.

Andy Truscott – Accenture – Member
I'm sorry, carry on without me.

John Kansky – Indiana Health Information Exchange – Co-Chair
Sorry, you were momentarily back so we could improve your reception we would appreciate your input. And we had Denise Webb. Welcome back, Denise.

Denise Webb – Individual – Member

Hello everyone. So, I was kind of listening, catching up. And I wanted to say that I'm in full agreement with all the points that Sasha made. And the point about a standard, obviously I'm not aware of any in healthcare, but having the military background, we did do security labeling, electronically. It's been a while since I've been out of the military. I imagine they have advanced quite a bit on that from a digital perspective. But we might gather some lessons from DOD on that.

John Kansky – Indiana Health Information Exchange – Co-Chair

Thank you.

Johnathan Coleman – Security Risk Solutions – Security SME

This is Jonathan.

John Kansky – Indiana Health Information Exchange – Co-Chair

Yes, please.

Johnathan Coleman – Security Risk Solutions – Security SME

I apologize. Which is to interact district interject on the point of reference. I know the term standard can be used differently, but there is an HL-7 standard, a normative standard for data segmentation for privacy. And within that is the definition of the value set for applying security labels to see CCDAs. So normal restricted and very restricted are called out in that normative standard. If that's helpful.

Andy Truscott – Accenture – Member

That's just CCDA, though. That would be CCDA, right?

Johnathan Coleman – Security Risk Solutions – Security SME

Yes, right. Yes, that's right.

David McCallie, Jr. – Individual – Public Member

And what's difficult to standardize, if I could jump in on that, is to any individual patient, a very different subset of the clinical data might fit into one of those labels. To say, this is very sensitive to me. I am an airline pilot for my visual acuity. It is very sensitive to me. I'm in HIV activist, an AIDs activist, and my HIV status is not sensitive to me. That's where it gets very tricky. It's not coming up the category but coming up with the mapping of the data to the category for individual patients.

John Kansky – Indiana Health Information Exchange – Co-Chair

Thank you. Noam Arzt.

Noam Arzt – HLN Consulting, LLC – Public Member

Yes. Just sort of for complete list, I just want to mention, other approaches to this have been conceived of and tried that isn't tagging. We did a project with UIUC, funded by one of the ONC sharp brands in the not too distant past. Where we sort of approached this not with tagging but as, essentially, a clinical decision support exercise? So in this case that we have a CCDA or an, I guess it was a CCD at the time, and the consent directive from a patient, could we redact a CCD based on patient's consent directive to remove the things that the patient doesn't want to share in that transaction. So, there's a very different of approach, because you want to end the document and to hope the recipient didn't look at what they weren't supposed to look at, right? I mean, to me there's something flawed on that whole approach.

So, there are other possible ways to do this. And frankly, I have never been convinced that the whole approach would ever work. That's just my opinion.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you.

David McCallie, Jr. – Individual – Public Member
The reason you need tagging in some cases is that the downstream behavior depends on where the data came from. So, 42 CFR part two restrictions on redisclosure. So, I agree with Noam's point, that it would be ideal for making these decisions at runtime based on the patient's current wishes, but you also need the tags in some cases for this other information other, although you can maybe that's provenance, really.

Denise Webb – Individual – Member
Well, there may be cases too where even though the patient doesn't want something shared, it has to be shared because the law requires it. So, then the tagging would have to come into play.

David McCallie, Jr. – Individual – Public Member
Yes.

Noam Arzt – HLN Consulting, LLC – Public Member
Well, in that case, maybe even the tagging is relevant. I mean if the law you have to share, that's it.

Denise Webb – Individual – Member
But then, what does the person who receives it, on the redisclosure. I think that's where the issue – where you first send it, then what are they allowed to do with it?

John Kansky – Indiana Health Information Exchange – Co-Chair
I can see where the two things are not – what are the patient wishes, doesn't determine whether the data is tagged not. It just depends on how you are using tagging when the roles are getting back to Sasha list of three. Andy, you have your hand raised again.

Andy Truscott – Accenture – Member
Yes, just quickly if you can hear me, I suggest we table these comments and let the task force work it through, hopefully. But what we use the term tagging, we just identifying, it's not descriptive as to how at this point. Just identify data and handle it appropriately.

John Kansky – Indiana Health Information Exchange – Co-Chair
And I think we have captured a fair amount of uncertainty which may be the key message for ONC, is that there is uncertainty. There's not a lot of experience. There's a lack of standards. And that sounds like maybe the kind of feedback that they needed, not to wimp out.

Can we transition any object is to transition to certificate authority backup and recovery? I will wait for a moment to give folks a chance to object before we move on. Meanwhile, I will direct people to 6.2.9, which is a mere one sentence. And I will try to remember how this got on the list, and they may have been Arien, who is not available with us today. But it may have been someone else. The one sentence which is again at 6.2.9. is that each QHIN who is an issuer of the certificate shall maintain backup copies of system, database, and private keys, to rebuilt in the certificate authority capability in the event software and/or data corruption. What I remember from the last time was, again it might be Arien or someone else who said I don't think that's a good idea at all. And here we are for discussion. David and then Andy.

David McCallie, Jr. – Individual – Public Member
Yes, I mean the question of whether QHINs should be certificate authorities is highly questionable. I'm not sure why you do that, number one. And number two, if you were an authority, you will have a whole lot more obligations than is captured in 6.2.9. By your certificate policy. Which goes on for hundreds of pages sometimes. So, I don't know why this belongs in there at all, frankly.

John Kansky – Indiana Health Information Exchange – Co-Chair
If you could extrapolate, you mean, because there are no requirements for a QHIN to be an issue of certificates, you are suggesting that having this one quasi-random requirement doesn't really fit, is that a misinterpretation of your comment?

David McCallie, Jr. – Individual – Public Member
No, that's pretty good. Quasi-random, I like that.

John Kansky – Indiana Health Information Exchange – Co-Chair
And thank you, David. Andy, something to add.

Andy Truscott – Accenture – Member
Yes, I agree with David. It seems a bit off in here. Was there a purpose of why this is was added? It does seem to me that if a QHIN is also certificate authority, then I would expect the certificate policy also to mandate – you know, I assume this is around **[inaudible] [00:37:28]** keys held in three remote places, so you can re-create the security world. If so, would make sense that does do that and doesn't deliberately enable that security world to be rebuilt. But that's the only thing I can think of as to why this is put in here in a quasi-random fashion.

John Kansky – Indiana Health Information Exchange – Co-Chair
Anyone presenting the ONC wants to comment on the rationale for why this is here?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
So, Jonathan I know it's on a fact-based question, but do you recall any comments or anything that pointed us to include this?

Johnathan Coleman – Security Risk Solutions – Security SME
No, I don't, I'm sorry. I really don't. Thank you.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
That's okay.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay well, so I sense we may have a recommendation. The politely says we suggest deleting this. Is that an overstatement?

Denise Webb – Individual – Member

And John…

Andy Truscott – Accenture – Member
And John, I think there's a reason here and that **[inaudible] [00:38:36]** for here, that if the QHIN is a CA, then it must – it's responsible for maintaining its own root keys. And it can't elect to manage the root keys and just delete them.

Denise Webb – Individual – Member
But what it be covered in their requirements of a certificate authority?

Andy Truscott – Accenture – Member
No, **[inaudible]**. Is just a policy, you can say **[inaudible]** keys, I'm not going keep them? We do that. I actually have some CAs where I cannot create in the security world. But I think that this is saying you have to do that. This is the one that you can't opt out of.

Denise Webb – Individual – Member
Okay. But it does seem rather orphan here because if you look at 6.2.7, the title of that is certificate policies. But when you read about what the sentence says, it's talking about the QHIN security policy requiring that the participant certificate meet or exceed criteria in the QHIN technical framework, and that's all says. So, it's almost kind of misleading where it says certificate policy. You kind of expect that you will read something my about if QHIN is the CA.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, I guess what I was hearing, and David, I see you have your hand raised. So, let me make a quick comment, and then we'll get to David. When I was hearing, was QHINs aren't required a certificate authority, but if they are, then there's a reason to have this in here. But there's probably a reason to have a whole bunch of other stuff, so if you just have this one thing, does that feel weird or incomplete? So is the recommendation, and I know we are going to draft these, but I'm trying to get as far down as we can. Our recommendation isn't taking this out, our recommendation that is, yeah maybe this is reasonable if a QHIN chooses to be a certificate authority, but it feels like one of several requirements that we would place on QHINs in that circumstance. And then, John Kansky would add, are we being too or is it necessary? David, and then Andy, again.

David McCallie, Jr. – Individual – Public Member
Yes, I think my hand was accidentally left up, but I would agree with what you just said. I think this is a technical detail that would be RCE area of responsibility. I'm not sure what the policy goal is here, to enumerate these particular subsets of requirements. I mean, if it could be translated into a policy goal, maybe that makes sense. But otherwise, leave it to the RCE to figure out specifics of the certificate policy.

John Kansky – Indiana Health Information Exchange – Co-Chair
So that changes the Kansky undiplomatic recommendation to take it out to leave it to the RCE, which is a more diplomatic version of taking it out. Is there pushback from Andy or others on that idea? An Andy, you conveniently have your hand up.

Andy Truscott – Accenture – Member
Yes. Actually, I am going to push back slightly. I think that this is here with a perfectly legitimate reason for saying, if you're going to be your own certificate authority, you make sure that you can recreate the

security world. And we can rephrase that as a policy objective, that's fine too. If I think through what RFC 3647 has around certificate policies, I think it is, the rest of that stuff, no, that's up to you to determine. Even CRLs. But this one, we don't want a certificate authority to be used if you can't recreate the **[inaudible] [00:42:47]**. I think we would all agree with that policy statement.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, I think earlier you called it a bit orphaned. Do you feel that other requirements would be on par with this one that is missing? Or not so much?

Andy Truscott – Accenture – Member
No. It's a bit orphaned when I look at the concepts of the rest of the TEF. The only thing I can think of, and David and Johnathan, you might want to comment on this, is around CRLs, certificate revocation lists.

David McCallie, Jr. – Individual – Public Member
I mean, to me this is just a narrow little sliver of a much broader problem, and I'm not sure I understand why this narrow little is in here. But I don't think it will cause any harm. I don't think anybody would remotely accept the certificate authority that didn't follow these rules. It's kind of like a no-brainer.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay, so I think there be a little bit of wordsmithing in the future. But to your point, not a giant controversy.

David McCallie, Jr. – Individual – Public Member
Yes.

John Kansky – Indiana Health Information Exchange – Co-Chair
Denise has her hand up.

Andy Truscott – Accenture – Member
Controversy.

John Kansky – Indiana Health Information Exchange – Co-Chair
Sorry if I said it wrong.

Denise Webb – Individual – Member
I was going to say that I liked Andy's version of the recommendation where instead of being so prescriptive here and tell them that they have to maintain backup copies of all these things, so rather than focus on the policy goal of being able to re-create the security environment if there is an event that causes corruption.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, I think we're capturing it. But I like that. It sounds like the recommendation is going to elevate this to a rational policy recommendation and leave the details to the RCE.

Denise Webb – Individual – Member

Right. And then where the RCE can specify what they're expecting them to be doing to re-create the security environment or have it in their policies.

John Kansky – Indiana Health Information Exchange – Co-Chair
It just likes 10 minutes of discussion, but I think I finally appreciate the sentiment group on this one. Anything else to comment before we move on to identity proofing and authentication? And while I'm waiting for a response, I'll direct folks to 6.2.4. Hearing no objections. My understanding, the identity proofing is – and I'm going to appeal to Zoe or somebody else. Is there a participant and participant member analog to 6.2.4? I'm fumbling through it now.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes, there is. I'm looking for it also. It should be 7.9… sorry. Yes, 7.9, sorry. 7.9 and 7.10 and 8.9 and 8.10. And then there's even another – it's basically just rewritten again in section 9, 9.3 and 9.4. But those are basically just rewriting of what was in the previous version.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, I apologize if I'm grossly oversimplifying, but it basically says that at each level, whichever the… that we need to add – it specifies I-AL2 minimum for identity proofing. And apparently applies at the participant, participant member, and QHIN level. Sorry?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay. My question was, and it may be answered, and I missed it, was, are we okay to accept the identity proofing of folks down the tree if we're a QHIN? Can a QHIN accept the identity proofing of the participant member handed to it through one of the participants?

Andy Truscott – Accenture – Member
I mean, it has to.

John Kansky – Indiana Health Information Exchange – Co-Chair
Yes. I mean, how can it be otherwise. So, is that assumption, is it stated overtly, and I missed it? Or is that just a completely rational assumption per Andy's comment? The question to ONC.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
I don't know that it got stated specifically anywhere, but I do believe that it's a rational assumption.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay. So, in terms of the right level, then I don't remember who posted the question. Is that a question of whether I-AL2 is sufficient or too stringent or does anyone have a comment regarding that level of identity proofing?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
So, I think the question came from Arien, and I might ask Jonathan to just like maybe give a brief overview of what those two levels require. I think Arien had a question on the previous call about just what the new version of the NIST, like how the new levels, the IALs, and the AALs compare with LOA

requirement to the previous version. And just wanting to double check and confirm that this these are the newest levels that we should be looking at.

John Kansky – Indiana Health Information Exchange – Co-Chair
Jonathan, is there any comment that you have?

Johnathan Coleman – Security Risk Solutions – Security SME
Not specifically. So, I think the identity assurance levels are described in this 863. And I-AL2 supports the real world existence of the claimed identity. So, I think that there is a sense there that that's a moderate degree of confidence that the person is who they are. And back to the earlier discussion of that, I think the burden is on the entity that is issuing the credential, making sure that that identity assurance level has been obtained at the time that the credentials are issued, whatever level that happens to be. Excuse me, whatever tier in the TEFCA organization happens to be. Whether it be a QHIN or a participant, for example.

John Kansky – Indiana Health Information Exchange – Co-Chair
And I, when I read this, and there's an example in the draft of for example what would conform to I-AL2. I was not familiar with the standard. I talked to our security guy because our organization has over 50,000 users. And he didn’t think it was unreasonable as long as we could as we did earlier, accept the identity proofing or our participants that wasn't – it would require effort. Maybe inclusion in participation agreements. But it was not necessarily problematic. Okay. So, it appears uncontroversial although, oh, Andy, can you tell me how to say that. Andy’s got his hand up.

Andy Truscott – Accenture – Member
Yes, I was just going to say we shouldn't comment around registration authorities and issuing authorities, and only marginally around certificate authorities because that’s detail about how this is implemented. I think we should just say that in the QHIN agreement with the RCE, there will be a trust arrangement made or something like that. Johnathan, you can say it better than I can.

Johnathan Coleman – Security Risk Solutions – Security SME
I think you said it very well. Thank you.

Andy Truscott – Accenture – Member
Well, you’re biased, old chap.

John Kansky – Indiana Health Information Exchange – Co-Chair
What about authentication which is also called out for comment here. And when Zoe was quoting 7.9 and 7.10, 8.9 and 8.10, there’s also 6.25, that they all are sort of pared. And it calls out for 8-AL2, which is an authentication level that I believe, among other things, implies two-factor authentications. Is that appropriate? Workable? Does anyone have a comment in that regard? I don't believe – well, while the industry is going to two factors, and people are getting used to two factors. That seems like perhaps a necessary, but perhaps a higher bar in terms of usability. I'm just talking to try to provoke opinion. Are we, is it, are we implying here that anyone, any participant, participant member, or QHIN, anyone who authenticates into what? Is going to be required to conform to AAL2, which is the two factor every time they log in.

Johnathan Coleman – Security Risk Solutions – Security SME

This is Jonathan. Just as a point. I think the definition of AL2 certainly does include multifactorial authentication, but it can include a combination of two single-factor authenticators, as well. So, there is I guess, wiggle room there, if you don't want to be doing two-factor authentications then.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. Andy.

Andy Truscott – Accenture – Member
So, wiggle room being **[inaudible] [00:54:33].** Just two instances of the same factor. Marvelous. Is there a national standard for authentication in healthcare environments right now that I am not aware of?

John Kansky – Indiana Health Information Exchange – Co-Chair
Was that directed to Johnathan?

Andy Truscott – Accenture – Member
Well, anybody who cares to answer. David, Johnathan, ONC people. Your gurus.

Johnathan Coleman – Security Risk Solutions – Security SME
I apologize, I didn’t hear the question. It broke up a little bit on me.

Andy Truscott – Accenture – Member
I’m asking, is there a national standard for authentication for health IT systems in the U.S. that I was unaware of?

Johnathan Coleman – Security Risk Solutions – Security SME
Not to my knowledge. I'm not aware of that off the top of my head.

Andy Truscott – Accenture – Member
So, there’s nothing **[inaudible]** or anything like that?

David McCallie, Jr. – Individual – Public Member
I think that there are some requirements and certification for EHR's and for patient portals to be able to support some of these standards. I'm not sure that there's an actual requirement that you use them. My concern here would be that the policy decision is whether or not accessing the federated records should have different required authentication and identity proofing then accessing any other record. So, for example, if I'm an individual exercising my individual right of access to a patient portal, I would have a certain standard in place, put in place by that provider's organization. If I go through a participant in a QHIN and through the TEF and get all of that data plus all the rest of my data in other places, should there be a need for a higher level given the potentially greater breadth of information be gathered?

And I think my personal answer is no, they should both be at a high level because the data is so sensitive. But I think that would be the policy question, is, are you trying to set a different standard that would be in effect for providers accessing their own records or patient accessing their own data segregated by a certain provider? I think this is consistent with how all access should be. So, this makes good sense to me.

John Kansky – Indiana Health Information Exchange – Co-Chair
Yes, my simplistic assumption in reading this was the authors of TEFCA wanting to say that we expect user authentication to be at this minimum level, whether that's the rest of the industry or not. This just makes good sense. That was my inference. Just echoing you, David.

David McCallie, Jr. – Individual – Public Member
Yes, I think this is an area where we will see a fair amount of change over the next couple of years. So NIST has I think very wisely left it in a form that doesn't specify which technology is used. We are going to see the proliferation of digital identities. The CARIN conference is going on as we speak about that. So, the technical standards will be changing, but requiring this abstract higher level of two factor makes good sense to me regardless of what technology emerges to make two factors easier to do.

John Kansky – Indiana Health Information Exchange – Co-Chair
And help me out anybody, I'm trying to develop my instincts, so in the world where the TEFCA ecosystems exist and are in place, it's a screening sort of a de facto – if one has two conform to an AAL2 authenticating users for anybody is going to have access to data in the ecosystem, you sort of de facto created that standard for anybody who's logging into any EHR or the patient portal, a HIE portal, etc. Because it's going not to make sense to have two levels of authentication. So, are we creating a de facto national floor for authentication by including this? Or did I go off the deep end?

David McCallie, Jr. – Individual – Public Member
Well, I think that it's not a bad thing to do that if that's a side effect that has. Although, given that at least for the near-term, the amount of data that will flow through the channels, TEF channels, versus the data that flows through other channels that won't be affected by TEF, I don't know that this tale will wag that dog anytime soon.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you, Andy, do you have a comment?

Andy Truscott – Accenture – Member
Blocking task force was very clear. We wanted to allow local organizations to have local deposers. And if those are the governing policies. So, I would suggest that whether the information is being sourced from near or from afar, it should be an approach to controlling access to that information. And then it's a decision for the QHIN and the participation agreement. So that allows organizations to connect depending on the security policies that they have on a local level.

John Kansky – Indiana Health Information Exchange – Co-Chair
Are you suggesting this is too prescriptive to the QHINs, or did I miss your point entirely?

Andy Truscott – Accenture – Member
[Inaudible] local organization that is…

John Kansky – Indiana Health Information Exchange – Co-Chair
Can you start over? You're breaking up.

Andy Truscott – Accenture – Member
I am agreeing with you. In the participation agreement between QHIN and local organization. And it's up to them to agree. **[Inaudible] [01:01:03]**

John Kansky – Indiana Health Information Exchange – Co-Chair
So, I'm detecting a perhaps different opinion district difference of opinion. On the one hand, I think I understand David to say this seems reasonable to state, and Andy, I hear you saying perhaps that it's too prescriptive, we are supposed to be trying to allow intra-QHIN policies to be set by the QHIN. Am I trying to pick a fight where there isn't one or –

Andy Truscott – Accenture – Member
David made a good point there, which is our we are treating data, which is out of my locally MR, different than data that's come from afar. There is nothing that says whether data is local versus foreign, that determines whether that data is more or less sensitive.

John Kansky – Indiana Health Information Exchange – Co-Chair
I completely agree.

David McCallie, Jr. – Individual – Public Member
Well, on the other hand, I think elevating finding a nationally sanctioned network, using a nationally sanctioned network based on the new law as a way to lift the expectation or access to the complete federated medical record makes a lot of sense. And if there are our local institutions who have lower standards, they probably we ought to worry about that.

Andy Truscott – Accenture – Member
And they shouldn't be connected to the national federated record.

David McCallie, Jr. – Individual – Public Member
Right. Because I can't meet the standards.

Andy Truscott – Accenture – Member
We agree. We agree on that. But you shouldn't have a different…

David McCallie, Jr. – Individual – Public Member
No, I think that we can't. We, ONC, can't tell those entities how to behave. They tried that in meaningful use and got it through. Maybe this is a chance to do it. To push a little harder on a national level. I mean do you access anything today without two factors. I can't authorize my Adobe Photoshop without two factors, for goodness sake. Surely your health records should be two factors.

Andy Truscott – Accenture – Member
David, if only every provider organization that I'm aware of believed as you do.

David McCallie, Jr. – Individual – Public Member
Well, that's why we are here.

John Kansky – Indiana Health Information Exchange – Co-Chair
I guess the observation or comment from, at least what my offerings would be his we are observing that this is not an inappropriate level, but that the industry may not be at this level yet. And so ONC has an awareness. We can agree that there shouldn't be two standards. That the standard that's suggested here is reasonable but acknowledging that it will drive some changes to the industry and

two factors is not there yet. There is some Kansky embedded in that poorly worded recommendation or comment. But others, I'm sure will fix it. Mark Savage has his hand up.

Mark Savage – UCSF Center for Digital Health Innovation – Public Member
Yes, I just want to repeat and confirm what David said about two-factor authentications. It may have been said on this. But the various privacy and security taskforces and tiger teams that have looked at this issue have all been at two factors. I think the question has been whether it would go beyond 2.5 or more. But definitely two factors. It seems it's hard to imagine how we can go backward.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. Andy's is back. Andy?

Andy Truscott – Accenture – Member
Sorry. I was on mute. I'm not supposing we go backward, Mark. My suggestion here is purely that they don't allow some kind of two-factor system to emerge, where access to local health records is somehow under a reduced level of integrity. So, access to third-party source health records. That doesn't seem to be what should we be doing here. Now I completely agree what we might want to say, okay, if you're going to be part of – if you're connected to a QHIN, then your local security policy needs to be the two-factor authentication. That I could go with. But not a two-track. That just seems wrong.

John Kansky – Indiana Health Information Exchange – Co-Chair
I think we're agreeing.

Mark Savage – UCSF Center for Digital Health Innovation – Public Member
So, when you say local do you mean internal?

Andy Truscott – Accenture – Member
I'm trying to not get into local versus **[inaudible] [01:05:59]** but the EMRs, the IUs on my desktop.

Sasha TerMaat – Epic – Member
I know Andy, I don't know if that participation in a QHIN should dictate anything about how the local EMR authentication works. And if folks want to implement a second layer of authentication for access to external data, they might have second layers authentication for access to defend data or for prescribing of the controlled substances or other actions, it doesn't seem like this is the right group to over prescriptively rule that out.

Andy Truscott – Accenture – Member
Agree, Sasha. However, I'm not sure that we should also be saying they should have a second level of authentication. Because there are a few usability aspects, then that would be of concern.

Sasha TerMaat – Epic – Member
So, I certainly think that we should be mindful of usability.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. So, what I hear the compromise position being, calling out AL2 is good. But not being prescriptive in terms of – we shouldn't create a recommendation that implies that that should also be applied locally. We should leave that autonomy open.

David McCallie, Jr. – Individual – Public Member

I mean, I think TEF has nothing to say about what happens locally outside the TEF. So, if a provider wants the portal to have no passwords at all, you will probably run into somebody upset, but would not be TEF for the RCE. TEF only pertains to participation in this particular network through these rules. Which is very different from what local decisions are around the patient portal. So, its moot point as to what the impact of this is on portals. I am just saying that just because some institution hasn't got the stomach to have the portal access, doesn't we should elevate the bar for the TEF, which is a new thing, and a much more powerful thing in the long run, because it's the whole record. And I don't think it matters. TEF doesn't affect what local institutions do. What they do locally, I should say. Just get the adjectives in the right place.

John Kansky – Indiana Health Information Exchange – Co-Chair

I understand. Andy.

Andy Truscott – Accenture – Member

I think it should be very cautious about this because we may well create these two tiers I'm talking about. And we want TEF to be something which is **[inaudible] [01:08:42]** to the end user. So that they can have a richer set of information around which to make clinical decisions. And putting extra authentication feet's in the way is not necessarily a smart way of getting a doctor **[inaudible]**.

John Kansky – Indiana Health Information Exchange – Co-Chair

I'm trying to listen and learn from the discussion. What I am hearing is, channeling Sasha's comments is yes it sounds like to levels is bad. But we are not going to tell – we want to keep usability, would consider usability having two different tiers of authentication is bad. So hopefully people won't be silly enough to do that. But at the same time, we don't want to, channeling Mark, to lower the standard below with what's been implied here. So, if you're going to reach inside the TEFCA ecosystem for data, you're going to have to meet the standard. If you don't have the stomach to raise your systems to that standard, then that's on you.

David McCallie, Jr. – Individual – Public Member

Yes, there's nothing wrong, yes this is David. I think particularly when it comes to privacy and security, there's nothing wrong with raising the bar. Particularly when you're really raising to community norms for all of the kinds of sensitive data. Your bank, your Facebook login, my goodness there are two factors everywhere now. I switched cell phones recently in this transition from work to retirement, and I had to set up, and we set up a dozen different two-factor accounts on the phone. It was a pain the butt. But that the norm now. Is there way technology will make that is in the future, but some we should shy away from holding access to you complete federated records to higher birth and perhaps the standards currently do.

Andy Truscott – Accenture – Member

David, no one is shying away from anything. I'm just not sure **[inaudible].**

David McCallie, Jr. – Individual – Public Member

I'm sorry, Andy, I need to make that sound prerogative. I just think two tiers, in some cases, when you're raising the bar is a policy goal, that's a good one. And in another case, two-tier is a bad one. If you have a network that's fractured because you can't always agree on network security protocols, that's a problem. If we get a higher bar of privacy for patient data, that's not necessarily a bad thing. I think we are probably close to agreeing, actually.

Andy Truscott – Accenture – Member
I know we are. And I can sound snarkier if you want.

David McCallie, Jr. – Individual – Public Member
Likewise.

John Kansky – Indiana Health Information Exchange – Co-Chair
We have descended into snarky. So, I think it's time to move on. Have we exhausted discussion of this particular point? I would assert that we have. Okay. We've got about five minutes before public comment. So, and we are now at tier 3. Let me prompt Zoe because I believe we talked about auditable events yesterday, but I don't want to gloss over that. Did we cover sufficiently on yesterday's call?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
We did cover auditable events on yesterday's call unless anybody has anything additional, they want to add that. Organizationally identity, I am not, we talked about it for a minute when we were going over the security provisions. But unless somebody in the group wants to remind us what they want to discuss there. I didn't have anything to add to that. And the last one was just noting that I have been taking on consent as a broader issue. Not in any particular prevision, so.

John Kansky – Indiana Health Information Exchange – Co-Chair
Got it. Is there any, so anybody wants to – all right. So, just let me give you a couple of options. Is there any rule that says we can't go to public comment a few minutes early?

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
No, you can go to comment right now if you would like John.

John Kansky – Indiana Health Information Exchange – Co-Chair
Why don't we take this break in the action to do that?

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Operator, can you open lines?

Operator
If you would like to be public comment, please press star one on your telephone keypad. A confirmation tone will indicate your line is the queue, and you may press star two if you would like to remove your comment from the queue. For participants using speaker equipment, it may be necessary to pick up the headset before the star keys.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Are there any calls in there?

Operator
None at this time.

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

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. So, Zoe or others, how should we make use of the last 13 minutes, I can open it and say okay, look at the list top to bottom. So, going back to tier 1 perhaps and say anybody who missed a call or woke up at 2:00 a.m. with a burning new comment that they hadn't made earlier. And prompt the group for anybody wanting to touch and on something we have discussed earlier. I will pause there for just a moment.

And while you are pondering that, I believe the expectation, and I need to get with Zoe and Arien, so don't hold me to this, although you may have to hold me to this. The intent is to take what we've got here and come up with a draft version one recommendation document, that we will circulate in advance of the June 11th call. And the June 11th call will be spent starting to hammer the draft comments into a progressively more final form. Zoe, is that consistent with what we discussed?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes, I think that that makes sense. So, we have a full workgroup call or a full committee call, I think, June 19th, where we were hoping in a place to present our draft recommendations. And then the last full committee call is July 11th. So, we can hopefully make the final recommendations then and vote.

I'll also add, we don't have any meetings right now set up right now for after June 19th. So, we will probably be adding meetings to people's calendars ideally, by the end of the day. And then I guess the last thing, I may be known to maybe provide a recommendation or comment on the public health things in TEFCA. I don't believe that we, I don't believe it until a long conversation about absence. Noam, and I know that there are some specific points that you wanted to make.

Noam Arzt – HLN Consulting, LLC – Public Member
Yes, I will try to do that. Frankly, it's difficult to look back at the matrix whose notes in the right-hand column are a bit cryptic or in some cases nothing there at all. And so, it's really hard to figure out what the task force talked about when I wasn't there. Just a point of comment.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes. So, we are doing their best to capture everything. So, I will remind everybody that we do have a cell team take notes after every call and posts them to the main HITAC website. So, you could take a look at those notes. This matrix is available on Google docs, and I believe the link was sent to the folks so you guys can take a look at the matrix. We also have transcripts from the calls, which I will be going over for the rest of the week and attempting, with John and Arien, hopefully, to clean up this matrix to make it a bit more readable and actually plug-in what recommendation we have heard and captured of the calls so far.

Denise Webb – Individual – Member
So, Zoe, are those transcripts available to you, and we just have notes on the web? So, like with Noam, I wasn't on several calls desperate because I was out of the country.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead

Yes, Katie, can we please send the transcript along with the notes. And of those being posted to the website?

Accel Solutions
Yes, they are.

Denise Webb – Individual – Member
Okay good. Thank you.

John Kansky – Indiana Health Information Exchange – Co-Chair
Mark, you have your hand raised.

Mark Savage – UCSF Center for Digital Health Innovation – Public Member
Yes, this falls in the category of perhaps a new issue, or perhaps I totally missed it and spaced on a previous call but jumping back and forth with the recent comment letters to ONC and CNS and TEFCA. I'm thinking about how standardized fire-based APIs might fit into TEFCA. As I quickly skimmed a few minutes ago to try to do some intelligence gathering, it seems like there are some leaning in that direction, because of the way things are going, but not a requirement. There's a reference someplace to place working with your existing infrastructure. So, I'm wondering if somebody could confirm what TEFCA does or doesn't say on that. And if it's not a requirement, to just put the question out there, should we be thinking about that issue?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Sure. So, I might put a note kind of to distinguish a little bit, when we talked about APIs, I think what we are really trying to distinguish between is document exchange versus a resource-based exchange, right? We currently in the TESCA and in the QHIN technical framework, we specify IHE profiles only. Of course, there can be IHE based APIs that support document exchange. So, I think what we are really trying to explore is sort of that distinction. Right now, and I think that there are purposes and value to both been able to exchange documents, like CCDAs, and also been able to just pull a resource or your med-list, for example.

Currently, the QHIN technical framework, it adopted what was already out there in the industry and what was found in implementation guides that are out there today. So, we basically took our cues from what's out there today, and what's being implemented already. We know that there are initiatives happening, like both common well and care quality, have convened workgroups around fire APIs. And so, we definitely do not want to trounce on that work. And ideally, as that progresses, that's something that RCE will be able to work with the industry to determine when it's ready to be added, whether as a requirement or just an allowance for QHINs to use. But currently as drafted, the QTF supports IET profiles only.

Mark Savage – UCSF Center for Digital Health Innovation – Public Member
So, I would just add as a placeholder that even if you don't feel the industry is there now, and I understand that, that now still might be the time to express an expectation for what's going to happen. So, you have a proposed regulation that talks about being ready by January 1st, 2022, for example. I guess what I'm putting up the right now is maybe this is a good topic for a short conversation or reflection in the future. I don't have my own thoughts made up about it. And I appreciate your summary so. That really helps. Thank you.

John Kansky – Indiana Health Information Exchange – Co-Chair
David has his hand raised. David, are you still there?

David McCallie, Jr. – Individual – Public Member
Yes, sorry. I was muted. An uncommon thing. I would just want to second what Zoe said. I think that logic makes a lot of sense. If the goal is to take advantage of existing networks and rope them under common agreement so they can keep doing what they are doing and doing a better for widely available connections, it makes sense to start with those document-based exchanges. I think that the pressure in the long run from the individual participants in the RCE will be a shift in the direction of more simpler API approaches, but I don't think anybody wants to start over before the first information flows through the TEF. That would be my argument or my position. It's good thinking.

John Kansky – Indiana Health Information Exchange – Co-Chair
Thank you. Andy.

Andy Truscott – Accenture – Member
Yes, I agree with David. I think we need to be thoughtful about how we will promote advancement as well.

Mark Savage – UCSF Center for Digital Health Innovation – Public Member
So, this is Mark. Just to ask, both of you think we shouldn't be talking now about whether to talk about a placeholder for the future? Is there a both and here?

Andy Truscott – Accenture – Member
I don't know, I was thinking.

David McCallie, Jr. – Individual – Public Member
I mean I believe that the only thing you would consider is saying don't do it. But since you're not saying don't do it, the RCE has been an authority, I think it would have the authority to work with the stakeholders and move in that direction. In other words, I think it will happen one way the other. I don't mind putting a statement in or something that says be aware of rapid evolution and in APIs. I think maybe more to the point would be aware of the new requirements from the Cures MPRM and stay consistent with those, so you don't make vendors to double work. And have to implement the same service in two different ways from scratch.

So, I worry more about consistency with the API requirements of the broader 21st Century Cures context that I do about TEF not getting to APIs. I think they will, or some fire-based APIs.

Andy Truscott – Accenture – Member
We need to make sure **[inaudible] [01:24:42]** with Cures. But what we don't inadvertently do is create some sort of testing ground where we continue with "standards" that may be less mature or less modern.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay, there are no more – go ahead.

David McCallie, Jr. – Individual – Public Member
No, go ahead, I'm done. That's enough.

John Kansky – Indiana Health Information Exchange – Co-Chair
And I'm just trying to bring us in for a landing. Thanks to everyone for the active dialogue. Much appreciated. We have got through the things we're trying to get through. Now the ball is squarely in the court of the co-chairs and ONC. And will turn on something that you guys can comment on. With that, Zoe, anything else or Lauren, anything else we need to touch on?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Nothing for me.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer
Nothing. Thank you.

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay, thanks all. I will talk to you next week.