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

Trusted Exchange Framework and Common Agreement Task Force

Transcript
May 23, 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.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Thank you. Good afternoon, everyone, and welcome to the TEFCA Task Force meeting. There's lots to cover, so let's get started, and I'll begin by taking roll. John Kansky?

John Kansky – Indiana Health Information Exchange – Co-Chair

Here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Arien Malec?

Arien Malec – Change Healthcare – Co-Chair

Good morning and/or afternoon.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Carolyn?

Carolyn Petersen – Individual – Member

I'm here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Aaron Miri?

Aaron Miri – The University of Texas at Austin, Dell Medical School and UT Health Austin – Member

Aaron Miri, here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Aaron, sorry. Thank you. Sheryl Turney?

Sheryl Turney – Anthem Blue Cross Blue Shield – Member

Sheryl's here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Thank you. Sasha TerMaat?

Sasha TerMaat – Epic – Member

Here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Steve Ready? Cynthia Fisher? Anil Jain? Andrew Truscott? Denisse Webb? David McAllie?

David McAllie, Jr. – Individual – Public Member

Here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Thank you. Mark Savage?

Mark Savage – National Partnership for Women and Families – Public Member

Good morning, here, and I have a question when you are finished with the roll call.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Got you. Noam Arzt? Grace Terrell?

Grace Terrell – Envision Genomics – Public Member

Here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

And Laura Conn?

Laura Conn –Centers for Disease Control and Prevention – Member

Here.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

Great, thank you. Zoe – Noam, what's your question? I forgot.

Mark Savage – National Partnership for Women and Families – Public Member

It was Mark with a question, and I'm noticing the agenda up on the meeting presentation, which doesn't look like the agenda in the slide deck for today. I'm just catching that.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer

No, we just changed that, so I'll throw it to Zoe so she can get us started.

Mark Savage – National Partnership for Women and Families – Public Member
Okay.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Actually, why don't I throw it to Arien so he can give the overview?

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer
Okay.

Arien Malec – Change Healthcare – Co-Chair
Yeah. So, I think people have noticed, at least I've noticed that we have not made as much progress as a task force as we did last time. And that's primarily due to the whole set of other activities that we all have going on, including the information blocking task force and the associated high-tech meetings, where we were able to finalize the information blocking task force recommendations. And we just haven't had had the ability to dedicate time, energy, and attention to the TEF. Since we've gotten through our tours and PRM recommendations, we're now in a period where we can dedicate more time to the TEFCA 2 Task Force.

But I think we also need to recognize that we're behind where we expected to be, and we're at risk relative to being able to make recommendations to ONC prior to the comment-close period. We may have to ask for an extension or allowance for that. What we're recommending at this point is, rather than do a deep dive on every topic, we want to make sure that we touch at least everything that's in our agenda for the TEF once at a fairly high level, and tag and note any topics that we think warrant additional follow-up discussion. We are going to try to get through those remaining items, particularly in privacy and security, today.

And then, tomorrow, the approach is to prioritize the work of the task force against the highest priority needs that require comments. So we've have already heard from the discussion a whole set of items that warrant future discussion and future follow-up. Rather than go deep on them in this meeting, our proposal is to touch privacy and security, make sure that we're tagging anything that warrants additional follow-up, and then create a prioritized list of items for deep discussion starting tomorrow. So I'm just going to pause there. John if you have anything to add to that overview of our suggested approach, A.) and B.) any of the task force members confused by where we are or hopefully accepting of the direction that we're proposing going in?

John Kansky – Indiana Health Information Exchange – Co-Chair
So, this is John. In other words, we are going to try and overview topics today, raise your hand as you have interest in saying, "I want to talk about X and dive into X more deeply," which we will put on a list of items to prioritize for diving into on future calls. So, rather than having big discussions today, raise your hand and note the topic that you want to nominate for discussion, if that makes sense. Comments please?

Mark Savage – National Partnership for Women and Families – Public Member
This is Mark. Makes sense to me. Just a question, that will also include things that have already come up in the past, right? We don't need to reraise them?

John Kansky – Indiana Health Information Exchange – Co-Chair

Yep.

Mark Savage – National Partnership for Women and Families – Public Member
Thank you.

Arien Malec – Change Healthcare – Co-Chair
You may need to reraise them, so we'll try to summarize what we think we heard from the task force and you may want to add other things to that list. But we're going to try to do our homework and make sure that we tag the most important items for follow-up discussion. And so with that, I think we want to turn it back over to Zoe and to Kathryn.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yeah, perfect. So, I'm going to do a brief overview of the privacy provisions, then I'm going to turn it to Alex Kontur, who's going to do an overview of security. And Kathryn, please feel free to jump in or add color or anything you wish as we go through this stuff. We are going to do it at a pretty high level.
So, first I want to say with the privacy and security section, just want to level that for everyone's understanding a little bit. The way that we drafted the privacy and security section was to align with and complement applicable, particularly the HIPAA privacy rules as much as possible.

So, the MRTCs are written with the assumption that everybody who is a covered entity or a business associate is currently following the HIPAA privacy and security rules. We go above and beyond then to say that QHINs, regardless of whether or not they are covered entities or business associates, must comply with the HIPAA privacy and security rules as if it applies to all electronic health information. And that's another little nuance there, the applying to all electronic health information, because what you'll notice is that the provisions that we've either mirrored from HIPAA or where we pointed directly to HIPAA, but we've actually written out in MRTCs themselves. We do that because, we want to apply those provisions to all electronic health information unless we say otherwise.

Also, a lot of the references that we make where we point directly to HIPAA, because we are expanding the requirements to apply to all participating entities in the TEFCA environment, again which would include non-covered entities and non-business associates. And there are certain exceptions in there. And actually, so one exception that I want to note right off the bat is that there's an exception for federal agencies, who currently do not have to follow HIPAA and they're following their own applicable laws. So, an example of that is the Social Security Administration. They follow their own applicable privacy and security requirements, and they would not have to follow any of the HIPAA requirements that we have put into the MRTC.

Arien Malec – Change Healthcare – Co-Chair
Zoe, sorry. I just want to ask a question or just make sure. What I think I understand is that in most cases, a HIN or QHIN would already be a business associate and already transacting data on behalf of the covered entity and in those cases, compliance with HIPAA would be required. There are cases where a QHIN may well be transacting data on behalf of a non-covered entity, and the intent of structuring it the way that the TEF does is to make sure that there's no ambiguity that everybody's basically holding against the same baseline rules.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes, that's a really good way of framing it, Arien. Thank you. And you'll notice we don't put the entire HIPAA privacy and security rule in here, right? So participant and participant members who are non-

covered entities and business associates, they don't have to do everything in HIPAA but we have very carefully chosen specific things that we do think are highly important in order to protect the privacy and security of the information.

So, one of the broader things that we're looking for comment from the task force is, first of all, our approach in how we have done this. And second of all, the sections that we have pulled from HIPAA, are those the right requirements? Are those the right provisions? Is there something that we're missing or something that you think would be too burdensome to put on those non-HIPAA entities? We're trying to achieve the right balance between protecting the privacy and security of the information that flows through the network, but still expanding the access of health information for all patients and providers.

John Kansky – Indiana Health Information Exchange – Co-Chair
And Zoe, it's John. Just to confirm, it's comply with the HIPAA rules called out as if they apply to EHI, true?

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

David McAllie, Jr. – Individual – Public Member
This is David. Just a quick comment, I think that some of the entities that would like to participate in this ecosystem would currently be regulated under Federal Trade Commission rules, and the industry has adopted this sort of notion that either you're under HIPAA or you're under FTC and depends on which, the rules are different. It would be useful as we go forward to clarify those boundary conditions here. And which actors are under HIPAA and which actors are under FTC, if that still make sense.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Absolutely. I am hearing an echo. Sorry, are other people hearing an echo when I talk?

John Kansky – Indiana Health Information Exchange – Co-Chair
A little bit.

Mark Savage – National Partnership for Women and Families – Public Member
This is Mark, yes.

Arien Malec – Change Healthcare – Co-Chair
If you are not actively speaking, please go on mute. Maybe that will help.

John Kansky – Indiana Health Information Exchange – Co-Chair
I'm sorry. I was just asking if David's question goes on the list of our approach?

Arien Malec – Change Healthcare – Co-Chair
Yes.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Okay, so If we could just make sure to capture that question in the notes, that would be great.

Arien Malec – Change Healthcare – Co-Chair

I think we've already captured the role of patient intermediaries. That was an item that came up last time in our recommendations, and I think it's an item that will come up for discussion this time, as well. So if you are worried about patient intermediaries, rest assured that we'll have time to discuss those points.

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

Okay, great. So, if we move to the next slide –

Mark Savage – National Partnership for Women and Families – Public Member

This is Mark, can I just throw in a question? To Arien's example that HINs and QHINs may already be business associates, but we're also talking about situations where somebody, there may not be a relationship and they must act as if HIPAA applies. There are some differences between covered entities and business associates, what role do they have to act as if?

Arien Malec – Change Healthcare – Co-Chair

They have to act according to HIPAA provisions lifted from HIPAA that apply to QHINs, independent of their status. I think we're going to go through those provisions in the rest of the conversation.

Mark Savage – National Partnership for Women and Families – Public Member

Very good, Thank you.

Arien Malec – Change Healthcare – Co-Chair

And as I said, I think as Zoe framed up, we want to make sure that the provisions that were listed are the right provisions. And then, Zoe, just to be clear, and Kathryn as well, my assumption would be this is not preemptive, that if I'm already a covered entity or already a business associate and covered by the terms from my covered entities, those terms would still apply. This is really just covering the cases where nothing else applies.

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

That is right, Arien. And we, in fact, in some of the provisions we actually spell that out and say, "This does not supplant your requirement to do a notice of privacy practices," for example. But, sometimes we do also say that if they satisfy the requirement through HIPAA , then that can serve as satisfying the requirement from the MRTCs. But in terms of governance, the RCE is going to be the one ensuring the compliance with the MRTC, not how it's done through HIPAA. But that's definitely something, I mean that's something I think that I would also say is on the table for discussion a little bit. So, if there is conversation about how that might work or in which cases, anything like that I think would be helpful to talk about.

Kathryn Marchesini– Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

And this is Kathryn. Thanks for that Zoe. The only thing I would add for consideration is to the extent, disagreement or the TEFCA broader discussion would be impacting or somewhat the appearance of disruptive to how things are currently occurring through business associate agreements, that would be helpful to understand as we look forward to the future.

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

Right, Thank you. Okay, so the first topic to review is the concept of minimum information. We brought this up briefly on the last call, and it's particularly applicable to Section 2.2.2, 7.2 and 8.2, which deal with the permitted and future uses of EHI. And so, basically we say that once EHI is received by a QHIN participant or participant member, they can retain, aggregate, use and disclose the EHI for anything that the individual has given explicit approval for, but only if the individual has received the minimum information about what is going to happen with their data. So, the idea here was that we wanted patients to not just receive a notice or a summary saying that their data was going to be used in some way, but we wanted them to actually have the meaningful ability to say, "Yes, I want my data to be used in that way," or, "No, I don't." And we wanted that to come across in an accessible and understandable way.

So, these are the items that we believe should be included in the minimum information when requesting patient consent to use their data for a way that's not one of the exchange purposes that we've explicitly stated in the MRTCs. And it needs to include items such as the person or entity that will be taking any action with the data; the specific purposes for which the action may be taken; how long; whether that EHI may be disclosed to any third party and, if so, to whom and for what purpose?; whether it may be used by a third party, and identify the third-party and the uses; whether the QHIN participant, participant member, and any third-party may disclose the EHI or – I'm sorry – and any third party to which any of them may disclose the EHI; whether the EHI may be sold or licensed; any material benefits or risks of such action; and whether the privacy and security measures set forth in the MRTCs will apply to the EHI that is the subject of such action.

We also, at the bottom we say that for purposes of this definition, they can't send a notice in all capital letters to satisfy the requirement that the minimum information be conspicuous. And that's something that we've seen done in the past and don't believe is sufficient in order to make this information conspicuous and acceptable to the patient.

Arien Malec – Change Healthcare – Co-Chair
These provisions that apply to the individual. Oh, go ahead, David. Sorry.

David McAllie, Jr. – Individual – Public Member
Well, that was going to be my question. It's I'm not exactly sure who this applies to in terms of the standard permitted purposes versus is this just for individual access outside of the standard permitted purposes? Zoe, who is required to provide this to the individual and when?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
So, whoever, whether it is that QHIN participant or participant member that's the recipient of the data, if they want to do anything with that data that's not one of the exchange purposes that we have listed in the MRTC. So if they want to use it for research or something else that's not part of the MRTC, so those seven exchange purposes, then they would have to send this notice to the individual who's the subject of the information getting their consent.

David McAllie, Jr. – Individual – Public Member
Yeah, I got it.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, Zoe, this may be worthy of going on the list for discussion. I was interested in some clarification. It may apply to – It's definitely 2.2.2, and the difference between Sub Bullet 5 and 6, 6 being the one that

says anything else you want to do, as long as you tell the individual minimum information, etc., etc., but 5 being you can do anything that's otherwise permitted by applicable law. So, just some clarification of, can I do stuff that's not illegal? Or can I do stuff that is not illegal as long as I get the individuals to take those steps in 6? Did that question make any sense at all? It was unclear to me, upon reading, whether you could do anything that the consumer agreed to as long as you'd given them minimum information, or the prior point, Point 5 saying or you can do anything that's not illegal. So I was just looking for some clarification.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
So, you can do anything that's permitted by applicable law. So, for example, if you are covered under your business associate, you can reuse and disclose the data for all of TPO, as opposed to the narrow set of PNs we have in the exchange purposes. But if you want to, I guess – I mean, research would still fall outside of this scope, I believe. Kathryn?

Kathryn Marchesini– Office of the National Coordinator for Health Information Technology – Chief Privacy Officer
Right.

John Kansky – Indiana Health Information Exchange – Co-Chair
But I guess that's a perfect example. Go ahead.

Kathryn Marchesini– Office of the National Coordinator for Health Information Technology – Chief Privacy Officer
Yeah, I think the intent is just because you tell an individual and they consent to it and it's illegal, that's definitely not the intent. I think, Zoe, what you are trying to articulate is to the extent that the use, if you want to use research as an example, if it's permitted under HIPAA to the extent you get the patient's permission, that still applies. But if there's other uses, TPO, as you know, TEF doesn't include all of them. I mean, if it's already allowed under law, that law kind of prevails over this agreement. I think that the goal is, as, I think, Zoe, you alluded to at the beginning, the intent was to zone in on areas that seem to be more, I guess, controversial, problematic, where we can try to standardize in some of the areas. And it's not to inhibit other exchanges that folks want to participate in just because it's not included in the agreement. To clarify, if that's at all helpful, I think in the future, we definitely don't want to send the intent of just because you got someone's permission, you're able to do stuff that is not in accordance with law.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, per the approach that Arien described in the beginning – I'm trying to avoid engaging in the discussion. I'd still offer that there's some questions to be asked there.

Arien Malec – Change Healthcare – Co-Chair
Yeah. And this question is purely for the purposes of just making sure I understand this provision. So, there may be actors that act on behalf of the individual that are participants under the TEF or are QHIN's under the TEF, deliver their data to the individual under the right of individual access, then the individual subsequently makes a determination about what they do and don't want to do. Under what cases would these provisions apply? And under what --? If you understand what I mean, there are these boundary conditions were sometimes I'm acting in Role 1 and sometimes I'm acting in Role 2. Does that question make sense? And I've got a specific example that if I'm a fruit company, as an example, and I do activity as a fruit company, both under the TEF as a participant and/or as a QHIN.

And I also build an app that allows the patient to make individual determinations about what they want to do on their data. At which point am I operating under the TEF and subject to these rules and in which point am I acting purely on behalf of the individual?

David McAllie, Jr. – Individual – Public Member

This is David. I would ask Arien's question in a similar way, contrast the constraints. If I'm an individual and I choose to use the APIs required under the data-blocking rule and download my data directly from a provider, how does the constraints of that access channel to my data differ from this access channel to my data, going through a TEF? Are there differences that this but additional constraints that says if you get the data through the TEF, you have to abide by these additional constraints that would not apply if you just got the data directly from your provider with API? By the way, I think these are good constraints. I like this. I'm just trying to understand where they apply and where they don't apply.

Arien Malec – Change Healthcare – Co-Chair

That's right.

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

Okay, so do we want to continue the discussion or should we keep trying to go through **[inaudible] [0:27:06]**?

John Kansky – Indiana Health Information Exchange – Co-Chair

Keep going.

Arien Malec – Change Healthcare – Co-Chair

Yeah.

David McAllie, Jr. – Individual – Public Member

Raise the question that's important.

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

Okay. All right, so if you go to the next slide. Okay, so first we include notifications around or, sorry, requirements around breach notification that apply to all QHIN participants and participant members as they apply to all of EHI. And we point specifically to 45 CFR Part 164 Subpart D as well as 45 CFR 1624.304, and also include anybody who has an obligation under the FTC rule with respect to any breach of security must also continue to comply with the FTC rules. And then, there's also a law-enforcement exception to the breach notification. So if the QHIN participant or member is notified by any law enforcement official that a breach would impede a criminal investigation, then the QHIN shall delay the notification for the time period specified by law enforcement.

The next section is meaningful choice, which is actually found in Section 2, instead of 6. Meaningful choice is a concept that applies – it's specific to the MRTC, so it's not something from HIPAA. But it is essentially in layman's terms, although we don't call it an opt-out, it is essentially a blanket opt-out of having the individual's data used and disclosed via the network. And, whoever has the direct relationship with the patient, so whether it's the QHIN participant or participant member, whoever's writing those services to the patient has a responsibility to provide the patient with the opportunity to exercise their meaningful choice, and also to display on their website, instructions for how the individual can go about exercising their meaningful choice.

Arien Malec – Change Healthcare – Co-Chair
Quick question there, I – Maybe David will ask exactly the same question I'm gonna ask, so I'll just defer to David.

David McAllie, Jr. – Individual – Public Member
I just want to register that we need clarity on when meaningful choice might not apply. For example, for direct treatment, is that clearly called out as exemption? Or does this actually change HIPAA rules?

Arien Malec – Change Healthcare – Co-Chair
This is **[inausible] [0:30:22]** HIPAA, right?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yeah, correct. It is not called out as an exemption. Unless something, like not exchanging, it would be violation of law, there are currently no other exceptions to meaningful choice.

Arien Malec – Change Healthcare – Co-Chair
So, the notion that – Go ahead, David. Sorry.

David McAllie, Jr. – Individual – Public Member
I got lost in the double negative there, or what sounded like that. If I meaningfully choose to opt out of my QHIN data sharing, does that stop any direct treatment sharing that HIPAA would allow?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
It would stop anything that's not explicitly required by applicable law. So that's stronger than just being permitted by applicable law. So, I believe the answer to your question is yes.

Arien Malec – Change Healthcare – Co-Chair
Yes, right. And then just as a clarifying question, the notion of meaningful choice was, I think, introduced by the Privacy and Security Tiger Team, although Devon may have taken it from someplace else. And the notion wasn't simply the ability to opt out, but the notion that rights and choice must be actually explained to the patient. And this is in accordance also with the information-blocking exceptions. So do I have that right? That not only – This is not a, "I need to offer an opt-out and if I offer an opt-out everything's okay." This is, "As a QHIN, I must make sure my participants let their patients know that they're participating, help them understand what that participation is and isn't, and give them the opportunity to give them the choice to participate or not participate based on the information that been provided to them." Do I have that right?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yeah, I think that is the intent. And we sort of combine the meaningful choice with the written privacy summary. So ideally, the entity would receive the written privacy summary explaining all of the rights around privacy and that would also include the instructions for how to exercise their meaningful choice. But, we would love recommendation for if we didn't quite hit the mark, or if we need to be more explicit in terms of how this is communicated to patients to really make it clear that they need to have this meaningful ability to understand what's happening with their data.

Mark Savage – National Partnership for Women and Families – Public Member

This is Mark. Back to David's question, I just want to confirm, if someone exercises meaningful choice and you've got direct treatment, you wouldn't be able to use the QTF for direct treatment, but you would still have the other mechanisms available, right? Meaningful choice is only respect to the QTF?

<u>Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead</u>
Or to the MRTCs or the common agreement as a whole.

<u>Mark Savage – National Partnership for Women and Families – Public Member</u>
Right.

<u>Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead</u>
You have an outside BAA that allows for that exception and, yeah, you could continue exchanging through that other contracting vehicle.

<u>Mark Savage – National Partnership for Women and Families – Public Member</u>
Right. Okay.

<u>David McAllie, Jr. – Individual – Public Member</u>
So, this is David. I think that's very unclear in the current document as to the sort of boundaries of what you can meaningfully opt out of for sharing. So I would just register that **[inaudible] [0:34:21]** concrete examples specifically around direct treatment.

<u>Arien Malec – Change Healthcare – Co-Chair</u>
Yep.

<u>David McAllie, Jr. – Individual – Public Member</u>
And that I want to just register a secondary point that we don't need to talk about now, but sharing the privacy preferences of an individual's meaningful choice action across a network in a robust way is not a very well-solved technical problem. So, just register that this is a challenging requirement to meet, technically.

<u>Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead</u>
Yes. Definitely – Go ahead.

<u>Arien Malec – Change Healthcare – Co-Chair</u>
No, Aaron just has his hand up as well.

<u>Aaron Miri – The University of Texas at Austin, Dell Medical School and UT Health Austin – Member</u>
I do. I have a few questions, actually, if that's okay if you guys can entertain me for a few minutes here. So my first question's related to meaningful choice as related to can I opt out as a patient? Is it opt out of everything or can I actually opt out of a way of the data being used? Let me give you an example. For research purposes, if I don't want my data being used for research but I want it being used for clinical treatment purposes, does that apply? Or is it all or nothing? Let me ask that first question.

<u>Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead</u>
The way it's currently written, it's all or nothing.

<u>Aaron Miri – The University of Texas at Austin, Dell Medical School and UT Health Austin – Member</u>

Okay. So that would need to be clear. No. 2, related to breach notification, it's quite possible these various QHINs, or whatever we're calling it now, could reside in different states which have different state jurisdiction related to breach timing, whatever else, 30-day, 60-day notification, those sorts of things. I understand we say here we have to meet all applicable law. That's totally fine. What about local law? Does this federal law supplant or replace the need for individual QHINs to know their local laws as well?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
No, absolutely not. So all applicable law includes all local, state, and federal law.

Aaron Miri – The University of Texas at Austin, Dell Medical School and UT Health Austin – Member
Right. And then three, related to mental health and substance abuse, how is that differentiated or bifurcated when it comes to choice and sort of that meaningful choice? Is there granular-level consent needed to be given as related to substance and mental health abuse? Because, as you know, even in clinical treatment purposes, you have to especially state you want that to be shared, even for treatment purposes. So, how does that impact my meaningful choice? Is it all or nothing there as well? Or is that another level of differentiation and we need to think about it?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Currently, as it stands, it's all or nothing. However, we are asking for recommendations and comments around standards or security tagging and confidentiality codes, as well a good format for communicating meaningful choice between the QHINs. And I think hopefully as it evolves and we start to work with the industry on more granular requirements in the QTF, that's something we're looking towards including. But actually, I'll defer to Alex **[inaudible] [0:37:22]** re-labeling.

Arien Malec – Change Healthcare – Co-Chair
Actually, let's just let a placeholder that one as a discussion point. I see that Mark has his hand up.

Mark Savage – National Partnership for Women and Families – Public Member
Just checking because I've seen this issue, if the individual exercises her meaningful choice somewhere midway and there's already some data being exchanged, is this draft clear about what happens with the data that's already in the system?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yes, meaningful choice is only on a prospective basis. So, anything that's already been used or disclosed, prior to the exercise of meaningful choice can continue to be used or disclosed.

Mark Savage – National Partnership for Women and Families – Public Member
So, it's not just a statement that cannot be purged from the system. You're actually allowed to continue using it.

Arien Malec – Change Healthcare – Co-Chair
It's a prospective choice.

Aaron Miri – The University of Texas at Austin, Dell Medical School and UT Health Austin – Member
But that also would interfere with any kind of right-to-be-forgotten components down the road. So, there's different things.

Mark Savage – National Partnership for Women and Families – Public Member
So I'll flag the question, Arien. What's prospective? Because you could say that the future use of prior data is a prospective choice. So it seems like there may be some clarity to **[inaudible] [0:38:49]** there.

Arien Malec – Change Healthcare – Co-Chair
Okay.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Okay, great. All right. Moving on to the next provision, it's minimum necessary. So, this one applies again to all QHINs, participants, and partisan members regardless of whether or not they are business associate or covered entities. And we specifically reference 45 CFR 164.514 D and we include exceptions that are set forth under the HIPAA rules, including disclosure of EHI to a request by a healthcare provider for treatment, disclosure to an individual who's the subject of the information, disclosure pursuant to an individual's authorization, or disclosures that required by law. Any questions on minimum necessary?

All right, next slide, please. Okay, 6.1.4, 7.4, and 8.4 titled "Other Legal Requirements," we could probably come up with a better name for it. But it mainly has to do with local consent, and local opt-in opt-out. So, basically, whoever has the direct relationship with the patient, whether it's the QHIN participant or participant member, is responsible for obtaining and maintaining copies of the individual's consent, approval, or other documentation when required by applicable law. So, if you have a state, like Rhode Island, that's opt in, the doctor that sees the patient in Rhode Island would have to have the copy of their consent, and they would be responsible for communicating that through to the applicable participant and QHIN.

Next we have the written privacy summary. Which, if you are any QHIN, participant, or participant member that offers services to an individual, must publish and make publicly available a written notice in plain language that describes their privacy practices regarding the access exchange use and disclosure of EHI. And the written privacy summary should eventually model the ONC model privacy notice, that we have on our website. And it should include a description, including at least one example of each type of exchange purpose that the entity offers. So, if you're a participant, and you offer individual access services and maybe quality assessment improvement, then you would make it clear that those are the two use cases that you're offering. It should include a description that provides the individual with a reasonable understanding of how to exercise their meaningful choice, so it should have instructions for how they can do that. And it should contact information for who the individual can contact for more information on the privacy policies. And again, this does not supplant the requirement to do a notice of privacy practices that meets the requirements of HIPAA.

And then finally, the last one is a summary of disclosures, which is our take on the accounting of disclosures requirement in HIPAA. And it's essentially the same as the accounting of disclosure requirement at 45 CFR 164.528 and it includes all of the same exceptions that are in there. So there are exceptions for treatment, payment, operation for an individual, for an individual getting his or her own EHI, an exception if there's an authorization under 45 CFR 164.508, and if there are any correctional or law enforcement reasons or national security or intelligence purposes for not providing the summary disclosure.

David McAllie, Jr. – Individual – Public Member
Question.

John Kansky – Indiana Health Information Exchange – Co-Chair
Go ahead.

David McAllie, Jr. – Individual – Public Member
It may be clearer in the text, and I don't have in front of me at the moment, but the disclosures happen at multiple levels and layers. So there's a disclosure from the participant to the QHIN, there's a disclosure from the QHIN to another QHIN, and then maybe a disclosure from that QHIN to the participant who did the requesting. To what level does this apply? Is this just a QHIN in-and-out? Or is it new rules on the participants? So, the individual can submit a request for their summary of disclosure to the entity with whom they have a direct relationship? And it would apply to what that individual has disclosed to the QHIN?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
To whoever they have had the direct relationship with, whether it's the QHIN, participant, or participant member.

David McAllie, Jr. – Individual – Public Member
But not necessarily what happens to it as it's slowed down from there or up from there, depending on the topology that you draw?

Arien Malec – Change Healthcare – Co-Chair
To ask David's question another way, does the accounting disclosure or summary disclosures apply to the activities of the organization to which the patient has a direct relationship and any QHIN that that organization may participate with? Or does that summary disclosures relate to any activity of any QHIN part is fitting in the TEF? Or is that a question that we need to frame up?

John Kansky – Indiana Health Information Exchange – Co-Chair
I think that is something to flag.

Arien Malec – Change Healthcare – Co-Chair
Okay.

John Kansky – Indiana Health Information Exchange – Co-Chair
And Zoe, I apologize if you covered it. On the summary of disclosures for applicable exchange purposes, is that the same thing one would account for disclosures for under HIPAA? Or are we saying all exchange-purpose transactions period?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
The exchange purposes, the applicable exchange purposes that are relevant in the MRTC.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, if I'm an individual, I have a direct relationship with a participant, any transactions with my data for exchange purposes would be captured in the accounting disclosure, even for PPO, etc., etc.?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
So, not for the exception. There's an exception for PPO. So, really it would only apply for, I guess, public health, benefit determination, and –

John Kansky – Indiana Health Information Exchange – Co-Chair
For the same things one puts in an accounting of disclosure under HIPAA currently?

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

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

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Here's the language on the screen. It took a minute, 9.5.3 has all of the exceptions.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
If I remember correctly, the intent behind this was not to try to broaden HIPAA in this case.

John Kansky – Indiana Health Information Exchange – Co-Chair
Yeah. In my opinion, that would be a bad idea, so I like your answer.

And then, a quick one – I think this is easy – going back to written privacy summary. Zoe, I understand you to say this does not supplant the need for a HIPAA notice of privacy practices, so does that mean that every covered entity that participates in the TEFCA ecosystem is going to have two privacy notices?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
It could mean that, although you could meet the requirements of our written privacy summary. If you have a notice of privacy practice already, then you could use that to meet our requirements.

John Kansky – Indiana Health Information Exchange – Co-Chair
So, you would just modify it to make sure it serves both purposes?

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

John Kansky – Indiana Health Information Exchange – Co-Chair
Got it, thank you.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Okay, are we ready to move on to security?

Arien Malec – Change Healthcare – Co-Chair
Let's do it.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Alex, it's to you.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME

Yep, thanks Zoe. Okay, so No. 1 minimum security requirements. This is something that Zoe covered a little bit in her introduction to privacy and security. This is one of those cases where we have applied certain requirement to non-HIPAA entities. So, just broadly, all QHINs are required to comply with all of the HIPAA privacy and security provisions as if they applied to electronic health information. And participants and participant members who are covered entities or business associates also have to continue to comply with the HIPAA rules that are appropriate to them or applicable to them.

However, if you are not a HIPAA entity, so not a covered entity or business associate, we have identified a certain set of security provisions or privacy and security provisions that you have to adhere to, and these do materially align with those found under HIPAA. So it's things like maintaining reasonable and appropriate administrative technical physical safeguards, protecting against reasonably anticipated impermissible uses and disclosures, protecting against reasonably anticipated threats to security or integrity of information, monitoring compliance among your workforce. And then also, as you determine the appropriate safeguards, each entity should consider things like its size, complexity, and capabilities, its infrastructure, the cost of security measures, and the likelihood and possible impact of potential risks to electronic health information.

Our next provision relates to controlled unclassified information, which is a certain category of information that's created by federal agencies. This NIST special publication 800-171, I believe, covers particular security requirements required for entities handling controlled unclassified information, and in this case, this provision only applies to QHIN level. We do not have a parallel provision for participants or participant members.

Arien Malec – Change Healthcare – Co-Chair

Quick question there. Many or at least some federal agencies treat EHI at higher than controlled unclassified. So, DOD treats PHI as readiness data, and appropriate to SRG HI. I don't know what DA does with regard to this, so… Anyway, maybe that's a placeholder for how do we align federal agency information security requirements relative to QHIN requirements?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME

Yeah, we don't have any specific provisions dealing with those rules and regulations. So again, I'd point to applicable law, and probably something that we might want flag for further discussion.

Arien Malec – Change Healthcare – Co-Chair

Yep.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME

Okay. Electronic health information use and disclosure outside of the United States. So basically, we have a provision here so that QHINs cannot disclose user-disclosed electronic health information outside of the United States, except as required by applicable law and if an individual user specifically requires that QHIN to use or disclose their information outside of the United States. There's also provision in hear about cloud-based service providers, which have to be physically located in the United States.

Arien Malec – Change Healthcare – Co-Chair

All right, quick question on that one. Why is this provision particular to cloud-based service providers? If I have a data hosting service or if I own my own hosting facility, can it be located outside of the United States?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
I don't think we specifically comment on that in this draft, so something to flag.

Arien Malec – Change Healthcare – Co-Chair
Okay.

David McAllie, Jr. – Individual – Public Member
Yeah, you need to define what you mean by cloud-based, something about where the servers are that manage the data or something, rather than a generic term like "cloud."

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
All right, next slide. Data integrity. Okay, so this is another one that applies to all three levels, QHINs, participants, and participant members, and they all need to include procedures that promote data integrity with respect to the exchange purposes under the framework agreements. There's a list of, I guess, five specific data integrity things that these entities have to account for.

So for example, procedures to safeguard that electronic health information is not improperly altered or destroyed; procedures to protect against reasonably anticipated impermissible uses or disclosures; procedures to main backup copies and systems, databases, private keys, software and data corruption, and that's related to performing a role as a certificate authority; procedures to test and restore backup copies of systems, databases, private keys for the retrieval of data in the event of a disaster, emergency, or any other circumstance requiring the restoration of electronic health information; and procedures to document methodologies and results of tests to restore backup copies of systems, databases, and private keys. And again, this is related to the role of serving as a certificate authority.

John Kansky – Indiana Health Information Exchange – Co-Chair
Quick question, this sounds to be mostly overlapping with HIPAA security. Was the intent that this was an element that went beyond HIPAA security? Or what was the intent?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Zoe, do you have insight?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Well, so it goes beyond in that it applies to all electronic health information but aside from that, it mirrors what's in HIPAA. One other small nuance that I would say is that I think for this one – or actually, I think this one you only have to do these processes for the exchange purposes that you…

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Perform, right?

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

John Kansky – Indiana Health Information Exchange – Co-Chair
So, I don't know if this deserves being on the question list, but where we've already said that QHINs, participants and participant members have to comply with HIPAA security as if it were pertaining to EHI. Did I make that requirement up, or did we say that?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
So, participants and participant members, if they're not covered entities and business associates, they do not have to comply with all of HIPAA. They only have to comply with the provisions we explicitly put in here.

John Kansky – Indiana Health Information Exchange – Co-Chair
And we're calling these out here? And that's the whole point?

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

John Kansky – Indiana Health Information Exchange – Co-Chair
Okay, thank you.

David McAllie, Jr. – Individual – Public Member
It's an enumerated list, right? Not the whole law.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Correct. So, the slight nuance that I was getting at a moment ago in that you only have to, for the data integrity provision and I think it's also the audit provision, which Alex will get to in a minute, you only have to do it for the exchange purposes that you perform. And our intention with saying that is so, for thinking about a third party app or a public health registry, that really only does one exchange purpose, one use case, then they only need to do the data integrity and the auditing requirements for that purpose.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Sorry, are we ready for the next one? Somebody asked me a question.

John Kansky – Indiana Health Information Exchange – Co-Chair
Yes, please.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Okay, authorization. So, not much else in the MRTCs beyond what's written here. QHINs, participants, and participant members must include policies to obtain written authorization. Well, they have to include written authorization procedures to confirm that any entities requesting access to system functions or electronic health information possess the appropriate credentials. So, we don't – Mapping this back to the QTF, we don't necessarily define anything about roles or anything like that. So, I guess the general policy here is that if you are a signatory to the common agreement or framework agreements, you are appropriately authorized to access electronic health information.

David McAllie, Jr. – Individual – Public Member
Does that mean that the definition of appropriately authorized is specified elsewhere, such as in HIPAA or state or local rules?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
No, it's mostly it's referring to some of the common access control concepts of role-based access and things like that. We don't define specific roles.

David McAllie, Jr. – Individual – Public Member
But you're essentially deferring the notion of what roles are appropriate to other regulatory frameworks, other regulatory constraints. You're not adding any new one. I get that, but that means it just defaults to what's already there.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Correct. Or if, for example, an organization delegates certain roles or authority under its own purview.

John Kansky – Indiana Health Information Exchange – Co-Chair
I don't know if anybody else agrees with this, but it strikes me that I understand why you've pulled out specific security requirements to make it a subset of HIPAA, but the nice thing about referring to HIPAA specifically is that there's a whole bunch of collateral and definitions and experience that everybody knows what that means. And so kind of to David's point, if I'm not bastardizing it, is that to pull these requirements out, freestanding, I'm not sure how clear it's going to be for compliance.

David McAllie, Jr. – Individual – Public Member
Well, this is David. That's certainly a fair statement of my concern but I think the context that it makes some sense to do what they did is that not everybody will otherwise be subject to HIPAA. So, you have to either re-enumerate them or make them subject to HIPAA, I'm guessing, from a regulatory framework point of view.

John Kansky – Indiana Health Information Exchange – Co-Chair
Or, and I'm not sure if what I'm saying makes sense, but as a compromise to do a whole bunch of this thing just like in HIPAA and that thing just like in HIPAA without having to – yeah. So, incorporate HIPAA security chunks by reference.

David McAllie, Jr. – Individual – Public Member
By reference, yeah.

John Kansky – Indiana Health Information Exchange – Co-Chair
Yeah.

Arien Malec – Change Healthcare – Co-Chair
It would be useful if I'm already subject to HIPAA, to be able to just defer.

David McAllie, Jr. – Individual – Public Member
But the place where this will matter is those non-covered entities that choose to participate in the QHIN will now have some new burdens placed on them, and it needs to be pretty clear what those things mean. The HIPAA will **[inaudible] [1:02:45]**.

Arien Malec – Change Healthcare – Co-Chair
I completely understand and concur with that. I'm just trying to avoid having to have double compliance efforts.

David McAllie, Jr. – Individual – Public Member
Yeah, totally agree.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
And just to be clear, this particular provision, I believe, some of the ones coming next, I don't believe they're actually covered in the HIPAA security rule. So if I'm wrong about that, please correct me. But this isn't referring to a HIPAA patient authorization or anything like that.

David McAllie, Jr. – Individual – Public Member
Right. Got it.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Okay. Identity proofing. This is based on the NIST standards. There's a suite of three guidance technical documents related to identity management. And so the requirement here is that essentially all entities have to be identity proofed at the NIST identity assurance Level 2 requirements.

All right, next slide. Authentication's pretty similar to identity proofing, also relying on the NIST standards, and requires all entities to be authenticated at the authentication assurance Level 2 requirements.

David McAllie, Jr. – Individual – Public Member
This is David. I ought to know the answer to this, but I'm not sure I do. And maybe Arien, you are closer. Would you think that these last two requirements introduce new burdens, compared to what participants in things like CommonWell and Carequality are already doing? Or are these consistent with that?

Arien Malec – Change Healthcare – Co-Chair
I'm a little confused by NIST Level 2. I thought that NIST went to a – changed its terminology in later guidance. And this is specific identity insurance, and not authentication. So, it might just be worthwhile in referring to the exact sections of the exact guidance, rather than say something like – and I assume you guys do that in the actual text.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
No, we do actually just refer to the guidance overall. I believe what you're talking about is that NIST originally had a sort of overarching assurance level, and the change is that they broke it down into these three subcomponents: identity, authentication, and I think maybe authorization. I'm not sure what the third is.

Arien Malec – Change Healthcare – Co-Chair
853-53 stroke three, is that right? Is that the latest?

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

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
And if I'm remembering -- go ahead.

David McAllie, Jr. – Individual – Public Member
My question was simply, is this an impactful change? Or is this just codifying existing best practices? And I am not expert enough to know, we would have to seek input from –

Arien Malec – Change Healthcare – Co-Chair
Yeah, sorry, you're talking about AAL 2, which is authentication. IAL is identity proofing, and I want to make sure that we understand what we are talking about.

John Kansky – Indiana Health Information Exchange – Co-Chair
Correct.

Arien Malec – Change Healthcare – Co-Chair
So which one are we talking about?

David McAllie, Jr. – Individual – Public Member
We talked about both of them.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
So, IAL would be the identity-proofing requirement and AAL 2 would be authentication requirement.

John Kansky – Indiana Health Information Exchange – Co-Chair
So I have a comment about identity proofing, which is that, it I remember correctly, participants can accept the identity proofing of a participant member and QHINs can accept identity proofing of participants. Is that correct?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Zoe, do you know the answer to that?

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
Yeah, yeah. Exactly. So the QHIN is responsible for identity proofing, the participants are responsible for identity proofing participant members.

John Kansky – Indiana Health Information Exchange – Co-Chair
And as long as somebody in the tree has done the appropriate identity proofing, everybody else can trust it is the better way of saying it.

Arien Malec – Change Healthcare – Co-Chair
As long as you're authenticating at every level. So, IAL2 is real-world identity proofing. David, I think that's consistent with Commonwell AAL 2 is two factor --

David McAllie, Jr. – Individual – Public Member
Yeah, the AAL 2 may be where there's more concern that that apply to individual access, and where two factor might not currently be in place. I think it should be, frankly. I'm totally in agreement with it. I just, I guess it would be worth looking for comments as to how it would be disruptive to the existing practices. And if so, is it justified?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Right, and identity proofing is more of a one-time event prior to issuance of credentials. Whereas authentication is something that has to happen on any request for electronic health information or request to send electronic health information.

John Kansky – Indiana Health Information Exchange – Co-Chair

Okay, keep going, please.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
All right, transport security. So again, all QHINs, participants and participant members must have written policies and procedures to ensure a secure channel for communications with other entities. And mapping this back to the QHIN technical framework, we have a requirement to use TLS, or propose the requirement to use TLS.

Arien Malec – Change Healthcare – Co-Chair
Nobody is not in favor of TLS. But with what cryptoalgorithm? Sorry.

David McAllie, Jr. – Individual – Public Member
Yeah, right.

Arien Malec – Change Healthcare – Co-Chair
1.1, 1.2, which cryptoalgorithms are included? Sorry let's please not include this. Let's defer all these naughty issues.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Arien, you're just showing off.

Arien Malec – Change Healthcare – Co-Chair
I am, it's true.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
There's another NIST document, I believe, that's included in that QTF. It's sort of a best practices document, or maybe it's an IETS document. I'm not 100% sure of the top of my head. But it does provide a little bit more clarification beyond the broad use of TLS. And I think we also version the use of TLS in the QTF.

Arien Malec – Change Healthcare – Co-Chair
Yeah.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Okay, moving on to auditable events. This one's a little complicated, because it sort of has a little mini flow down baked in. Because QHIN in its security policy has to identify a set of auditable events, and then the participants and participant members essentially pick from those auditable events with appropriate modifications based on the transactions that they perform.

Arien Malec – Change Healthcare – Co-Chair
Let's flag this one for discussion, because I think it is odd to have MRTCs that refer to QTFs that will change.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Fair enough. There's also, in this provision, some minimum information that an auditable event must include, such as the description of the event; date and time; success and failure; and then, where appropriate, the entity that was responsible for the event.

Arien Malec – Change Healthcare – Co-Chair
Just so I'm clear – Yeah, go ahead, David. You probably are going to ask the same question.

David McAllie, Jr. – Individual – Public Member
Maybe. I'm just trying to relate this to the accounting for disclosure requirements. Auditable for whose review and under what circumstances? Linking those together seems reasonable to understand how they – who gets to see these auditable events.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Right, so there is some language in here that the entities must maintain an audit log, including records of all of these events, and must make it available during any audit.

John Kansky – Indiana Health Information Exchange – Co-Chair
By the RCE?

David McAllie, Jr. – Individual – Public Member
Yeah, who is doing the audits?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Not specified, so something to flag, perhaps.

Arien Malec – Change Healthcare – Co-Chair
Yeah.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Okay, next slide. Security policies. So, each QHIN security – or, sorry, certificate policies. Each QHIN security policy has to require that all participant certificates meet or exceed applicable criteria. The QTF does not have very extensive criteria at this point. We didn't necessarily want to dictate how security or certificates were assigned and distributed in this network.

Arien Malec – Change Healthcare – Co-Chair
Yeah, okay. So we talked about individual identity assurance. We haven't talked about organizational identity insurance. Do the MRTCs talk about organizational identity assurance? Because that tends to be actually much more important.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
I believe that the NIST specification applies to both. But again, that might be something worth flagging.

Arien Malec – Change Healthcare – Co-Chair
Let's just flag this one. Yeah.

David McAllie, Jr. – Individual – Public Member
This is David. I agree that details of this should be deferred to the RCE and stakeholders, but will caution that it's a thorny area when you bring federal partners in and mix networks. Just historically, it's been sometimes more complicated than you might expect to get agreement on certificate policies.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME

Okay, security authority backup and recovery. So each QHIN who issues certificates must maintain backup copies of systems, databases and private keys in order to rebuild the certificate authorities capability in the event of software or data corruption. This should not be read to imply that a QHIN has to issue certificates, just in the event that they do.

Arien Malec – Change Healthcare – Co-Chair
I think it's an extraordinarily bad practice even to include this section. So, just flagging this one for note.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
All right, finally we have security labeling. Let me just – So, this is not included in the MRTCs at this point. This is part of introductory language. We did include a proposal related to security labeling that we are requesting comment on. And, basically, the idea here is that in future iteration of TEFCA, data holders would have to apply security labels for any electronic health information that includes codes from value sets indicating one of three categories of sensitive information: mental health, substance use disorder, and HIV. Additionally, all electronic health information pertaining to minor patients would have to be labeled.

Arien Malec – Change Healthcare – Co-Chair
By the way, I'm looking at SP 800-63a. It does not refer to the extent that I can identify to organizational identity assurance. It really talks about applicants, biometrics, and the like. So, just as a point that I think we need to talk about organizational identity assurance.

John Kansky – Indiana Health Information Exchange – Co-Chair
And is this – Go ahead, David.

David McAllie, Jr. – Individual – Public Member
Just a question on the security labeling. I didn't pick up when I read the document that you're saying this is preamble, but not part of the actual MRTCs. Does that mean it would be deferred to the RCE to work out in the future in conjunction with ONC? Is that the intent? Security labeling?

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Correct. I believe – Zoe, correct me if I'm wrong – based on comments that we get, this might be incorporated into a future version of the MRTCs, so that wouldn't necessarily involve the RCE establishing a policy, but ONC establishing a policy.

Zoe Barber – Office of the National Coordinator for Health Information Technology – Staff Lead
That's exactly right, Alex. So, if it's in the MRTCs, that means ONC established the policy. If it's in the ARTCs, then the RCE wrote it. So I'd say we reserve the right, for the **[inaudible] [1:17:28]** the common agreement, after this public comment period to add something about security labeling in MRTCs.

John Kansky – Indiana Health Information Exchange – Co-Chair
And just for my own understanding, I did not hear you reference compliance with CUI as a reason for security labeling. Is that not one of the reasons for this? I want to make sure I'm not connecting two things inappropriately.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
Correct, that would not be a requirement under the proposed policy.

John Kansky – Indiana Health Information Exchange – Co-Chair
But you are asking for – You listed a bunch of proposed categories for which security labeling might be useful in the future, but I didn't hear you say CUI. My understanding is that part of the challenge of organizations complying with appropriate NIST standards is figuring out how to security label the data. I might be confused.

Alex Kontur – Office of the National Coordinator for Health Information Technology– SME
No, that's correct. The proposed policies do not make reference to CUI, and from my understanding, one of the issues surrounding CUI is labeling. So, maybe something to flag as another potential use case for the security labeling policy.

David McAllie, Jr. – Individual – Public Member
This is David. On that thought, I like the idea of separating labeling from actually respecting what those labels imply that you do. But, I would caution you that without going that second step, you might not have achieved whole lot of good. So at some point, you have to actually say – you have to handle the label data in special ways, not just label it. And that's the hard part is governing secondary use of the data, or even secondary redisclosure or things like that, 42 CFR2 and stuff like that. The easy part is labeling. The the hard part is figuring out what the rules are about what you must do to respect those labels. But separating it into two steps makes a lot of sense to me.

John Kansky – Indiana Health Information Exchange – Co-Chair
And I see that we're being gently reminded that we've reached public comment.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer
Yes, thank you. Operator, can you go to public comment please?

Operator
If you'd like to make a public comment, please press *1 on your telephone keypad. A confirmation tone will indicate your line is in the queue. You may press s*2 if you'd like to move your comment from the queue. For participants using speaker equipment, it may be necessary to pick up your handset before pressing the star key.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer
Do we have anybody waiting in the line for public comment?

Operator
None at the moment.

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer
Okay. John and Arien?

John Kansky – Indiana Health Information Exchange – Co-Chair

So just as a time check and progress check, is it reasonable or is it irrational to try and circle back to stuff like modalities and exchange purposes, to add items to the list for prioritization? Or how do you want to use the remaining time?

Arien Malec – Change Healthcare – Co-Chair
Did we get through all privacy and security requirements?

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

Arien Malec – Change Healthcare – Co-Chair
Okay. What I propose since we only have six more minutes, is that we end a little bit early. We've got some follow-up time, and I propose that we assemble a list of high-priority items, and then review them with this group tomorrow. Maybe a solicited call for, "This issue is burning so hard in my pocket that I can barely stand," if you've got some things that you don't think that we're sufficiently aware of. Otherwise, I just propose that we review the list of high-priority topics, and with the team tomorrow, and then get agreement that that's the right list, and then we prioritize that list and work through and chunk through in priority order.

Sheryl Turney – Anthem Blue Cross Blue Shield – Member
That sound like a good plan.

John Kansky – Indiana Health Information Exchange – Co-Chair
Sounds good.

Mark Savage – National Partnership for Women and Families – Public Member
And that list, Arien, will include past items, too? This is really helpful to see the discussion notes on the right. So, just checking.

Arien Malec – Change Healthcare – Co-Chair
Yeah, the discussion notes is a great practice that we should've been doing a while back, but we'll continue to do.

John Kansky – Indiana Health Information Exchange – Co-Chair
So we need to capture previous items and add them to this list is what I heard?

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

Mark Savage – National Partnership for Women and Families – Public Member
Yes, please. Individual access services for me at least.

Arien Malec – Change Healthcare – Co-Chair
Yep, and I assume that David will concur with me that the overall architecture is exchange. The specifics of the QTF also need discussion. We also heard about the role, and this may be individual access services, but the role of individual intermediaries, and their obligations.

David McAllie, Jr. – Individual – Public Member

Yep. And I think the secondary use question around – oh, no. Secondary use, maybe we talked about some of those questions, but there was another one about reciprocality of an aggregator of patient data.

Arien Malec – Change Healthcare – Co-Chair
Yep that is right.

David McAllie, Jr. – Individual – Public Member
That was an unanswered question, like what duties do they have to not respond or can they opt out of responding if they evacuate?

Arien Malec – Change Healthcare – Co-Chair
And then, yeah, so do we have the right bundling of exchange modalities? We had some flags for discussion of directed exchange or pushed exchange. And the obligations of QHINs to do those. I'm still just confused by when and in what circumstances are QHINs required to do all exchange modalities as opposed to part of exchange modalities. We have a lot to discuss. We're going to go off-line, assemble a list, and then review that with this team tomorrow.

John Kansky – Indiana Health Information Exchange – Co-Chair
Great, thanks so much.

Arien Malec – Change Healthcare – Co-Chair
Thanks, all.

David McAllie, Jr. – Individual – Public Member
Sounds good.

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

Cassandra Hadley – Office of the National Coordinator for Health Information Technology - Acting Designated Federal Officer
Thanks.