



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
February 11, 2015**

Presentation

Operator

All lines are bridged.

Michelle Consolazio, MPH – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Standards Committee's Transport & Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Dixie Baker? Lisa Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Hi.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Aaron Miri?

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas
Hello.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Boban Jose? Brian Freedman? Jason Taule?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems
I’m here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, Jason. Jeff Brandt? Jeremy Maxwell from ONC?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology
Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, Jeremy. John Hummel?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District
I’m here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, John. Lee Jones?

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health
Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, Lee. Peter Kaufman?

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, Peter. Scott Rea?

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
I’m here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Scott. Sharon Terry? Steven Lane?

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Steven. And do we also have Julie Chua on the line from ONC?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yup, I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Are there any other ONC staff members on the line?

Mazen Yacoub, MBA – Healthcare Management Consultant

Hi, Mazen Yacoub is here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Thanks, Mazen. And with that...

Mazen Yacoub, MBA – Healthcare Management Consultant

Thank you.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

...I'll turn it back to you Lisa. Lisa, are you there?

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Sorry, I was on mute, I was already talking. Thank you.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Okay.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I wanted to say welcome to everyone on the workgroup and to those listening in the public today. This is a meeting of the Health IT Standards Committee's Transport and Security Standards Workgroup. Today we have one objective and that is to do a review of the Interoperability Roadmap in order to help equip us to do some review tasks that we're going to hear about from ONC today. So, we will be hearing from

ONC staff on various portions of the roadmap, our...the questions that are being asked for us to address in this workgroup, our work plan and our timeline as well. So that's what we're going to do today.

Yesterday there was an in-person meeting of the HIT Policy Committee and the HIT Standards Committee, so a joint meeting and at that time, we had a briefing on the Interoperability Roadmap from Erica Galvez and on the standards advisory document from Steve Posnack. Those were very informative and there was a lot of interaction with the committee members, some questions and then some initial comments. I think very informative for those of us on the committee. We are going to revisit some sections of that roadmap today, assuming there are a lot of you that haven't been on those calls. This is specifically for us, for this workgroup and to help enable us to be ready to work on our tasks and our questions from ONC with regard to the privacy and security sections of the roadmap.

So with that, I think I'd like to first of all see if there are any questions from the workgroup members on the scope of the meeting today, and we'll revisit what you heard at the end and see if we're all on the same...all have the same understanding of our task and work plan going forward. But at this point, are there any questions or comments? Okay, so we have on the line today several folks from ONC and I think on the line are Julie Chua, who is lead IT specialist for...in the Office of the Chief Privacy Officer and Jeremy Maxwell who is an IT security specialist in the Office of the Chief Privacy Officer. I don't think we have Lucia yet, but she will be joining us later. Lucia Savage is the Chief Privacy Officer at ONC and she's also going to join our meeting and have some conversation with us as well.

So Jeremy at this point can I turn it over to you?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Ah yes, that would be great.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

All right and Michelle, if you could switch over to the slides, we'll start with the first slide. Could you back up maybe three slides or so? Ah, yes...and then the next one. There we go, great. Sorry about that. So thanks everyone for joining the call today and what I'm going to do is walk you through a high level overview of the Interoperability Roadmap, just spend a few minutes on that and then zero in specifically on the sections that the Transport, Security & Standards Workgroup has been charged with commenting on in the roadmap.

So I think everyone has seen this slide, the FACA milestones and we are right there in February, the Interoperability Roadmap has just been released as you all should be aware of and we are going to start reacting to that. So you can please advance the slide.

So this is a slide that was presented yesterday at the joint meeting that has the HIT Standards Committee work plan for all the various workgroups. So if you can't read that small text down at the bottom on the next slide, I expanded that. You can go to the next slide, please. So here is our task and date as it relates to the roadmap. So you can see at the top line, here we are on February 11, we are

doing an overview of the Interoperability Roadmap and we're going to reserve the next couple of meetings to have discussion around the roadmap so we can make sure that all of your comments are heard and captured and then the comment period is closed on April 6. And then on April 22 meeting of the Standards Committee is when the comments will be presented to the Standards Committee. If we can go to the next slide.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Jeremy, I have a question about that, can you go back?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Sure.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

This is Lisa Gallagher. Umm, so the comment period closes for the public on April 6. Between April 6 and April 22, the time of the Standards Committee, are we still working on our comments or do they have to be completed by April 6 as well?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Lisa, this is Michelle. So, because our committees are so special to us and guide us on so many things, we often give them a little bit more time than the public, just because you're consolidating and coming to consensus across your groups and you're kind of tied to the meeting time. So, you'll be given a little bit more time, just based upon when the Standards Committee falls.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay and so then the April...what is the first meeting of this workgroup in April and can we use that meeting as well, Jeremy, that's, I think, a question for you, to finalize our comments?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes, absolutely.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And do we know what the date of an early April, or even the end of March meeting that we have that we can add to this list of dates.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes, we have a meeting March 25...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Um hmm.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

...and April 8 as well.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, can we add those two dates on here and figure out, um, you know, I'd imagine the 20 whatever of March we would still be working on finalizing and then what...how could we utilize April 8, that would be helpful.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Lisa, this is Michelle; I do want to make one more comment, though. We'll have to figure out when it happens, but at some point the Certification Rule and the Stage 3 Rule will be released and so we'll need to manage the timing of that and the comment period for that as well. So, there could be some overlap and we might not want...we'll have to figure out, if we finish this work beforehand, is how we transition over to that. So, just something to keep in mind.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, I think that's fine and we can talk about that when the Chairs meet in our planning call. So thank you. Okay Jeremy, I'll turn it back over to you. Thanks for indulging me in that question.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yeah, no worries. All right, so we can go to slide 5, the next slide. All right, so you can see where we are in kind of the roadmap process. So the roadmap has been released and, as we just talked about, when the comment period end and then we're targeting sometime in the middle of the year to release the 1.0 Version of the Nationwide Interoperability Roadmap based on all the public comment we received, including the comment from this workgroup. Next slide, please.

So I think everyone understands why we are talking about interoperability as we know kind of where we are in the healthcare timeline, we've done a good job with digitizing healthcare in this country, now we are ensuring that that information can flow freely in a private and secure manner across the healthcare system. Next slide.

And this slide was presented yesterday at the joint meeting as well and so, if you haven't had a chance to look at the roadmap, the roadmap is broken into kind of three phases where the goal of the first phase over the next couple of years is to ensure that we have nationwide ability to send, receive, find and use a common clinical data set. And then building upon that foundation in the preceding years we'll expand the interoperable data, users and sophistication kind of building on that initial framework and then in 2021-24 will be expanding that to a broad scale learning healthcare system. And there are cross-cutting concerns and requirements that run across all three of the phases, as you can see down at the bottom. And you can see that privacy and security is integral to that. Next slide, please.

And as we were developing the roadmap, there were a couple of principles that we, guiding principles that we used as we were going through the various pieces of the roadmap. And as you can see,

protecting privacy and security in all aspects of interoperability is one of the foundational principles that we used to guide the development of the roadmap. Next slide.

And drilling down just a little bit more into the cross-cutting requirement for the learning healthcare system, you can see that privacy and security is throughout, requirements number 2, 3, 5 through 10 or 7 through 10 all have security and privacy at their core. Now, these requirements map to specific sections in the roadmap and what we've done is, we've charged each of the workgroups with specific sections in the roadmap, because obviously the roadmap is a very large document and to the conversation, we don't have all the time in the world, right, we only have a certain number of workgroup meetings between now and when the comment period closes down. So we wanted to help focus efforts to make sure that we had appropriate coverage of each section of the roadmap. You can go on to the next slide.

So with that, the Transport & Security Workgroup has been charged with roadmap Section E, which is ubiquitous and secure network infrastructure; Section F, which is the verifiable identity and authentication of all participants and Section G, which is consistent representation of permission to collect, share and use identifiable health information. Those are the three sections that we would like the TSSWG to focus their efforts on.

If you have other comments on the roadmap outside of these sections you're certainly free to follow the public comment process and submit those comments outside of the workgroup, but within the workgroup we would like to focus our efforts on these three sections. And as we go through these sections, there are a couple of general questions and specific questions that we'd like your feedback on.

So more generally, we'd like to know, are there actions proposed in the draft Interoperability Roadmap, are they the right actions? And will they advance the interoperable nationwide healthcare system in the near term, while moving down the road towards the learning healthcare system. And are there any gaps, things that we missed, that we need to address? Are the timings listed in the roadmap appropriate? Are we being too optimistic or do we need to pull in some dates because we can accomplish them sooner? And are we engaging the right stakeholders for each of the critical actions? Those are some general guiding questions to keep in mind as we go through our conversation. You can go to the next slide.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Excuse me, can I ask a question? This is Lisa.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes. Sure.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Maybe this is for you or maybe Julie or Michelle but, the topic of provenance, did we...did any group get assigned that work?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes they did. Michelle, do you remember which group?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, I just want to make sure it didn't fall off the table.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes, it is not within the purview of the TSSWG, but there was another group, Michelle, do you recall which group that was?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

I don't know off the top of my head, I'm sorry, Jeremy.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Okay, no worries.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yeah, but we'll make a note of that, Lisa, and make sure that we share that with you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

All right.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Great. And then more specifically, so we have the general questions that we want you to keep in mind as we go through each of the sections and then for each of the sections we have some specific questions that we would like your feedback on. Obviously you're free to comment on other things within these sections, but these are some of the things that we specifically want your feedback on. And we'll go through each of these questions as we cover each of the sections.

So for the next part of the presentation, we will dive...do a deep dive into each of the sections that are assigned to the Transport & Security Workgroup and Julie is going to cover the first section.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Great, thanks Jeremy and thank you everyone again for joining us. This is Julie Chua and I will be going over the Section E, which is the ubiquitous secure network infrastructure. And if you could advance to the next slide, please.

So of course we all know for interoperability there has to be a stable, secure and widely available network capability and we emphasize in the roadmap that it should be vendor neutral, of course, and should support a wide variety of core services. So within this workgroup, with regards to cybersecurity, the charge or the specific question, in addition to the high level questions that Jeremy just went over, is that we would like the TSS Workgroup to give us some...their input and recommendations on anything that the federal government specifically should focus on first to move towards a uniform approach to enforcing cybersecurity in healthcare.

And we emphasize that we need to keep in mind the HIPAA and the CEHRT rules as well as the possible new cybersecurity legislation that is supposed to come out and we need to be mindful of those and specifically also, are there frameworks, methodologies, incentive programs and anything else that healthcare as an industry has not considered but should. Any questions about that? Okay.

So for encryption, the specific question and charge for this group is to identify if there are any other gaps, aside from the lack of policies and guidance for implementing encryption in technology and standards for encryption. So, we want to know...we all know that encryption is not being implemented right now widely, as it should; so we are asking this workgroup to see and to identify any gaps or any other reasons for that lack of adoption.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Julie, this is Lisa.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Is there a reason for the parenthetical phrase, you know, can you explain why that's in there and what you exactly mean.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Oh, meaning the aside from lack of policies and guidance?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Okay, so we all know that HIPAA does have requirements around encryption, right? And the CEHRT Rule for 2014 edition, we do have encryption in there also. But given those policies, are there other things that we should be looking at, other gaps, because it seems that those are not enough drivers for encryption...is it because people don't know how to use them? We don't have the technology or the standards to use them? Or like those are the things that we would want this workgroup to deliberate on. Does that help?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

It does, but it seems like you're excluding us from saying, we could use more guidance, right? I mean, you're saying, that's obvious so don't list it or something, I think that is probably an area where we're going to want to identify gaps. So...but I'm not sure if we're being limited from doing that.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

I would say no, we just wanted to note that we understand that there is that lack of policy and guidance already, but if we feel that the workgroup has certain recommendations around that, then of course we do want to hear that and document it and make sure that it gets captured.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

This is Scott...sorry, this is Scott Rea and I was...

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Go ahead, Scott.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

...I just wanted to make a note here that it would perhaps be better if that language said, including lack of policies and guidance for implementing encryption.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Exactly.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

In other words, you're recognizing that it's the case.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Sure, sure. Jeremy, is there anything you wanted to add to that? I'm actually making a note of that change.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Actually, so this is Aaron Miri, I do want to add something to that, Julie. I think he hit the nail on the head. I heard your comment that HIPAA requires encryption and while that...it doesn't actually say it, it kind of lists it as addressable...

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

...an organization could choose to do a risk analysis or risk acceptance and say hey, we're not going to encrypt, we're going to do all these other mitigating factors instead because, I don't know, it might...there might be a biomedical device that won't work with encryption on it so we're going to put a lock and a shock collar on it or whatever. So there could be other extraneous factors that force an organization to not encrypt, not for any other reason than the fact that they can't.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

So is there going to be a rewrite of the HIPAA Security Rule that actually says you must encrypt, no matter what?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Umm, I...ONC cannot speak for OCR on that matter, but I do stand corrected on that but what I was trying to come across is, there are certain standards addressable or not in HIPAA and the Breach Notification Rule, right...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Uh huh.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

...regarding encryption; so, we do know that there are some policy drivers out there, or incentives to do this. But...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas

Oh, absolutely and I agree with you 10,000 percent, Julie. And in fact, I have brought it up a number of times on these calls, which I’m glad are all recorded and you can go back and hear them, that I think one of the biggest needs to encourage provider organizations, such as myself, to make the investment in encryption, and to do those kinds of things, is to give air cover and to show that you’re not being negligent so if in the event you do have a breach, you’re automatically...you’ve tried your darnedest. There’s a...you’re not going to get...the potential for a finding of being negligent is very slim to none. So I think some sort of acknowledgment and respect of, okay, organizations who have done everything they can do are given some sort of air cover, I think that’s going to be very helpful and encouraging.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Thank you for that. So I just wanted to make sure that Jeremy, you are okay with this or any other comments you needed?

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

One other comment, this is Steven Lane. I think similar to the idea of air cover, you mentioned incentive programs here, I think the idea of some standards in terms of what could or should be done in response to security breaches or violations by either organizations or individuals would probably be helpful. I don’t know if the time for that has come; I know in our region we deal with...we get input from the Attorney General, from the Office of Civil Rights, from other groups and organizations. I think having some more standard disincentives, if you will, might be helpful in the long term.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

This is Lisa. So I think those are all really good comments and these are the kinds of recommendations we will want to develop in our subsequent meetings. So Jeremy, can...if...I guess Julie was asking if you’re okay with a change of wording here for our task and then we can move forward with your slides.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes, I’m fine with that.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Okay, great.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

So the next slide please. Okay. So this slide shows what you all will see in the roadmap. We do have critical action sections in each of the bigger categories within the roadmap and for cybersecurity, I just

want to go briefly through these five critical actions for the next couple of years, to give you all an idea of what we were thinking.

So ONC will work with OCR to release an updated Security Risk Assessment tool and hold appropriate educational and outreach programs. We have also identified that we will continue to coordinate with ASPR, which is the Secretary...Assistant Secretary for Preparedness and Response on priority issues related to cybersecurity for the public health...critical public health infrastructure. And in relation to that is our work to continue to support and enhance a single health and public health cybersecurity iSAC.

And that is something that we are currently working on and we are making sure that we do identify that as a critical action for the industry to know, as well as the cybersecurity framework and how it really is relevant to the health and public health sector. We are trying to work with NIST and OCR to make sure that we do provide additional guidance on how the HPH sector can utilize that framework. And the last one is for HHS to work with the industry to develop and propose a uniform approach to enforcing cybersecurity in healthcare in concert with enforcement of the HIPAA Security Rules. I think number 5 is really key and that's why that is one of the main supporting questions that we are asking of this workgroup that we need feedback on and input on as to how we can tackle that. Any questions on this slide?

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

Julie, this is Brian Freedman.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yes.

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

How much input are they going to allow us to provide for the ONC risk assessment tool to get it updated or modified or I guess, however you want to put it?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

The risk assessment tool that is always open for public comment and feedback and we can make sure that this workgroup has that email or that contact information for feedback on the risk assessment tool. We are really trying to make sure that we do an update on that, because we do get some feedback on how we can improve it, so we certainly...yes. We welcome...yes.

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

Um hmm. Okay. Okay great, I just...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So this is Lisa...

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Oh, sorry, go ahead.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I'm sorry, is the last question done because I can hold my question, because I'm having a little trouble hearing.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Did that answer the question?

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

I'm good, thank you.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Great. Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So Julie, my question is more in line with the clarification of the scope of our tasking here. My understanding of the roadmap is that the document contains critical actions for everyone in healthcare, not just the federal government. So the ones that are listed on these slides, they're...they each pertain to actions of the federal government. Are these the only ones you're asking us to comment on because you need feedback on what you all...your actions or is there a reason why we're not commenting on other actions of other parties?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Okay. So specifically for cybersecurity and encryption, you will see that it has a lot of the critical actions for the next two years are focused on what ONC and HHS is currently already doing. So it goes back to the higher level question that we have with, are these the only things that we should be doing within the 2 year period, right? These things are what we would like industry to know, these are happening right now; however, if this workgroup says, you need to add 6, 7, 8, 9, 10 to two years, then that's feedback we would really appreciate or we would need to hear.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so that would include actions that we could assign to the industry as a whole or standards bodies or HIEs or other players or is it just ONC?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

That is right, it's something where we would welcome, if you know or if this workgroup identifies an SDO needs to do this work, a trade association, a private sector organization needs to do this; then we need to know that.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman. I think that was a great point about the rest of the industry. This is something that can't be limited just to government programs and have the pediatricians kept out of that because they don't take Medicare and a lot don't take Medicaid, things like that. One of our points should be to determine ways to get buy-in by the entire community, all stakeholders, not just stakeholders dealing with the federal government...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

(Indiscernible)

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

...because it only works if everybody does it.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right. Yes, exactly; thank you, Peter. Because one of the higher level...or the broader questions for this workgroup is, are the right actors and stakeholders associated with the critical actions, right?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

So that is something that we really would like to hear from the workgroups in general...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And so that's something we can consider when we go through our discussions at the subsequent meeting.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And in fact, I would also add that we should think in terms of other levers that are available to us and what actors can be engaged with regard to the levers. So let's say there are requirements for participation in an HIE, could we use that as a lever to move the industry on cybersecurity; those kinds of things where we think creatively about how we can move things forward and not just with regulation or guidance from ONC and OCR.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Absolutely, Yes and Lisa, thank you for giving that comment because that is a key thing for the workgroup to realize and understand is that we are not limiting this to just federal government, or ONC for that matter, yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Thank you.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Thank you. Any other questions?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Hey Julie, this is Jeremy; I just also want to add that you can see in years...from 2018 to 2020 and 2021 to 20...that should be 2024, that we are also looking for feedback on those...you know, phase 2 and phase 3 of the roadmap as well. So be thinking about...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Jeremy...

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

...what could occur in those...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

This is Lisa; with regard to those out years, is there nothing in the roadmap document for those years because I know that we had stakeholder input in the fall and I'm quite sure that people gave...suggested critical actions for those two time periods, so I'm just trying to clarify, do we have no critical actions in there and you're just opening it up for input again? Or did they reject some of the input and think it wasn't workable? I mean, do you know the history of that?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

I personally don't know the history; I can research that and get back to you on that. I do know that these tables were...I pulled these straight from the roadmap document, so that this is how these tables appear in the roadmap.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Thank you.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

So we can move on to the slide...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Actually Julie, this is Aaron; I just want to ask one quick question and this may be just off-center and I apologize, I'm just trying to make sure that I get my facts straight. So today a lot of you probably got the news bulletin about the new Cyber Threat Intelligence Integration Center, the CTIIC, which Washington is now starting for counter-terrorism and sharing of information; is that...that's different than this ISAC, correct? Or is it the same thing just different mechanisms for information sharing?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Well the straightforward answer there is, we are trying to make sure that we have a robust infrastructure for information sharing, right? So with this new one that is being set up, I am sure that whatever we come up with at HHS will be feeding into that or part of that workflow. Because we can't just set something up where we are not either part of DHS's NCCIC center, we can't just stand something up without everything else flowing to and from that ISAC or the ISAO that we are trying to set up.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Gotcha; so I'm glad you said that because I think there might be some value in somehow very quickly or concisely saying that this will be part of a larger...

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

...information sharing so that everybody's benefitting from the collective, right? So if you think of a beehive, this is one little cell of the beehive, you're not on an island in the middle of nowhere; so we're able to see trends because you're going to have to really give a lot of assurances to providers, including my own organization, to share data that could be somewhat competitive knowledge and if you have an issue, there might be somebody in town who could use that and try to capitalize. So, I mean, there are

going to be a lot of things to work through. I'm just saying upfront, it might be very...it might be beneficial to mention something like that.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Great. Thank you. Yes and we do want to make sure also that it's not misunderstood what we mean by information sharing versus threat information sharing and I think that's a lot of the issues that come up with that and what you just said was, people not wanting to share because there may be certain types of information or data that they wouldn't want to share. So we're trying to make sure that that is clear.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Excellent. Thank you.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

You are welcome. So anything else on slide 14? Great. All right, slide 15, please. Okay, so for encryption, for the next two years the critical actions that we have provided, and again, these are ongoing ONC efforts and we welcome additional feedback on other things that we should be looking at in the near future. And for number 1 it is, working with OCR and the industry to develop "at rest" standards for data encryption and provide technical assistance. And OCR is...or will consider whether additional guidance or rulemaking is needed. And number 2 is the same; it's just for the "in transit" standards for data encryption.

The third action is ONC to continue developing guidance for implementing encryption policies or...because one of the things that ONC, I'm sure everyone knows is, we are educating...an educating body, right, and we coordinate. So that's one thing that we try to continue and we want to make sure we continue with encryption because that is something that we always hear that people or our stakeholders do not know how to implement encryption policies or do not know how to implement encryption, period. So that's number 3. And number 4 is, ONC working with payers to explore the availability of private sector financial incentives that increase the rate of encrypting and starting discussions with insurance carriers who offer cybersecurity insurance.

So, any questions on that? Great; and with that I turn it over to Jeremy and again, thank you so much to all the workgroup members. I really appreciate the feedback that I've...that we have gotten already and we really look forward to your expertise and your experiences to guide us and make sure that we capture everything that we should to make this work. So, Jeremy?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Thanks, Julie. So the next section is the verifiable identity and authentication of all participants and you can go on to the next slide. So the requirement that this section is built on is that legal requirements and cultural norm dictate that participants are known to the system so that the system can verify the accesses to the data and the services is appropriate and that this requirement goes across all participants in the health system, so it includes providers as well as patients and individuals, system administrators, technicians, those types of roles as well.

So the specific charge here is what identity proofing and authentication standards, policies and protocols can we borrow from other industries. Other industries have been electronic for a little bit longer than healthcare has, things like banking and finance, social media or email; are there standards or policies, protocols that we can borrow from those? Or are there healthcare specific things that we need to be addressing? So any questions on the charge before we get into the specific critical actions under this section? All right; we can advance the slide.

So here, under policies and best practices, there are a couple of critical actions around the concept of multifactor authentication. So we know that this has been a topic of discussion across the industry is where multifactor authentication should occur or can occur and how mature the technology is that supports multifactor authentication. And we also know that there are other areas of healthcare that are looking at multifactor authentication and so we want to make sure that we harmonize any multifactor authentication that we adopt as part of the roadmap with those other efforts; things like the DEA electronic prescription of controlled substance standards, which requires multifactor authentication, is as an example. And we also want to make sure that identity proofing is covered in the roadmap as well, because identity proofing is the entry point into the system.

And if there are no comments, we can move on to the next slide. And around standards we want to work with health IT developers to leverage the existing technologies to provide efficient and effective paths for identity authentication and proofing. And standards development organizations, we're also asking them to work with health IT developers to conduct pilots using RESTful approaches for authentication.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Jeremy, this is Lisa. Can you explain number 1 a little better? When you say leverage mobile technologies and smartphones, are you saying that once we figure out the requirements for multifactor authentication we want to encourage developers to deploy those things using mobile technology and smartphones? Is that what you mean?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Ah yes, it is. And so the...our thinking here is that mobile provides an accessible way to do multifactor authentication. So there's, for example, for my email, I have multifactor authentication through my phone on my email where it requires my username and password as well as a code...if I...whenever I log in to the first time to my email on a particular computer or device, it texts a code to my phone and requires me to punch that in, in addition to my username and password. So it's an accessible way for me to do that multifactor authentication. That was our thinking behind that critical action.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

But, it's not to the exclusion of multifactor authentication on the hospital network or something, I mean...

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Absolutely, yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

...because...

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes. Absolutely, that is not to the exclusion of any other technologies, and there may be other better technologies out there and certainly that can be a topic of discussion in the workgroup if there are things that we're missing or things that, you know, how we should tweak this; we definitely want to hear that feedback.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Right, and this is Aaron Miri and I'm not a lawyer or any of that, I'm just looking at this and trying to put different hats on, especially from a technical perspective and I think we might want to be careful as we say smartphones, because a smart device might be classified different than a smartphone, and it might be a smart watch at some point and it might be a smart whatever and you start really narrowing the ability of people to be innovative using different things.

To your point, there might be a better technology in two years that Apple or somebody comes out with and you also start really segmenting the market from being able to develop on things because you talk to any developer that's a mobile device developer and they already will complain about the speed to which they can release a new version of an App and how slow it is and how costly it is at times. So just some food for thought that we might want to think through the wording of this and I like the perspective, I really do, but I can see a lot of people having some heartburn over this.

M

This is...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman I think that those are all good points and I think we should...more devices, but another thing I'd like to put in here is to determine methods of evaluating the security of the...built into the device. One of the things the DEA has put into the interim Final Rule is that you can't use the same device as your two-factor authentication end to prescribe on because they think that the device can be hacked. I would really like to have a way of determining if the devices were...had strong enough security so that they could be used that way and being able to share that with the DEA.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

All good points and I appreciate everyone's input. So Jeremy, I don't know, you know, this is the wording that's in the document so we can, as a workgroup, take this wording and identify all of our challenges with it and our suggestions as part of our workgroup exercise, correct?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes. We would welcome that feedback.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas

It is definitely encouraging though to see the direction of the path. I mean, it’s absolutely the right direction, so I just...I appreciate everybody commenting. It’s really good stuff.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yeah, thanks for the feedback, it’s good to know that we’re at least on the right path. All right, so any other comments around the verifiable identity and authentication of all participants section before we move on?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I think we’re good, Jeremy.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

I’m sorry, go ahead.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I...this is Lisa and I was just saying, I think we’re good to move to the next slide.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Okay. Great. So the last section that the TSSWG is charged with is the consistent representation of permission to collect, share and use identifiable health information. Now this section is actually one of the few sections in the roadmap that multiple workgroups were assigned to it and I’ll explain, as we start to go through this. We can go on to the next slide.

So the Privacy & Security Workgroup and the TSSWG were both assigned to this particular section because there is some overlap in both of their workgroup charters as it relates to this particular section. The Privacy & Security Workgroup is going to be looking at this from a policy perspective and the TSSWG will be looking at this from a standards perspective. And so as we get into the critical action, there will be critical action that we will leave to the Privacy & Security Workgroup to comment on and there will be critical actions that we’ll focus the TSSWG on; and that will become clear as we walk through this.

So this particular section, the requirement has built on is that we need to be able to capture consistent representation of the permission to collect, share and use identifiable health information. And the charge to the TSSWG is, we would like to know what standards should we put forward in the 2016 Standards Advisory for basic choice. And so as you know, there’s...with the roadmap there’s a standards advisory that accompanies it that outlines the kind of best of breed standard for various things. And in the 2016 Standards Advisory we would like to include basic choice standards in that, but we need your feedback on which standards we should put forward for that.

In addition, we want to know, how much work ONC should be doing on other standards while clarifying permitted uses? And so if standards development needs to be done, what should...what's the priority of things that we should be working on? Is it data segmentation for CDS? Is it data segmentation for privacy? Is there something else entirely that we should be working on from a standards perspective?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And Jeremy, this is Lucia Savage. Hi everybody, I'm sorry I'm late, I had two prior conflicts. Just to clarify a little bit about that basic choice question, we've been getting a lot of questions about that. We had a very astute one yesterday at the joint FACA, for those of you who could attend, which was, are we saying everyone should be offered basic choice or if you're going to offer the choice of sort of opting in or opting out, to use the old language, how should you do it? And it's really the latter; it's a standard for how to do it if you as an organization decide that that's what's appropriate for you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Lucia, this is Lisa Gallagher. So how...so the term basic choice, I mean you just equated it to opt in and opt out, but I think...how does ONC plan to socialize the use and definition of that term so we can all be answering the right question?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Umm, it depends a lot on some preceding work set forth in the roadmap and I don't want to derail Jeremy's important question, because we want to make sure we're asking you guys the right question then give you a chance to ruminate on it. But we've really kind of lined out in the roadmap this three layers; the bottom layer is permitted uses, right? No actual piece of paper from an individual is required for access, use and disclosure when it's a permitted use.

And there are a few of those that are really core to the ordinary functioning of a healthcare system; I'm not talking about law enforcement, but really what happens in the care process, in the payment process and in the quality improvement process. So, really focusing on those and those things are what the rules are right now, right? But we have a manifestation where people have offered choices when they didn't have to and we want to bring standards to that activity. I don't know if that clarifies...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

...and if you guys read over it with this context and the feedback back to us is, this is as clear as mud, go back to the drawing board, that's the purpose of the public comment period.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

And Michelle, could you advance the slide, the next slide talks about basic choice and granular choice. Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman and this is a serious question although I think that the answer is already known; is there any way for a federalized mandate to override the state's individual requirements for this because it is going to make it extremely hard for a national interoperable system to have every state have very different regulations that are almost a different language from one another?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Well that's...I mean, that's one of the things we'll be looking at, to be honest with you, because some states have passed statutes and of course they are entitled to pass statutes that add protections on top of HIPAA and that's the way the law works. And other states have enacted policies or in fact, the policies are really manifest through contractual document that don't even rise to the level of a State Executive Order. So there are a lot of different ways that states have done this and some haven't done anything at all.

And so...and, on top of all that, there are a lot of different technical ways that people have implemented the information capture about a choice. And so this is really about the information capture about a choice; we don't...all our office can do generally is explain to people the consequences of going down one path or another path. We're really a great explaining organization, we have a lot of great experts between you guys on our workgroups and our staff; but we don't change...we don't write HIPAA rules, we don't change statutes and we don't tell states what their laws should be, to be honest.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

And Lucia, this is Aaron Miri and I would see...let me try and explain it. So I was trying to explain this to my wife, who's not an IT professional, I would say it's no different than when you sign up to be a donor when you get your driver's license, do you want to be a donor or not? And you'll check a box and record you're data; it would be something like that, right?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Exactly. It's very simple for this binary situation, it's not...so in the roadmap we have the second thing, and it's reflected on the slide which is, granular choice and that gets into all these particular clinical conditions that states also have; we're really just talking about the binary choice, in or out...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Yup, okay. Thank you.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

...exchanging or not exchanging.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

So, this is Jeff. So you're saying we're going with opt in...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

No.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

...that's what that...that's what that means if you have a binary choice and it's a blank box, that's opt in.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Well it's actually not because under the background rules, information is able to be exchanged without your choice at all so it's about how those two things work together, right? How the background rules that we have in place work and what happens when a person makes a choice...a personal choice to override the background rules.

So if I could analogize, it's going to sound like it's really off, but just trust me on this for a minute, because I've been using this analogy a lot and it resonates with most people. So most of us, I mean we have families, we may have assets and property, we may or may not have a will. If we don't have a will and you die tomorrow, there are a bunch of rules that take care of your property. The will...the purpose of the will is to say what you want to do that might not be specifically in those rules, that might be changes from those rules; write it down in a will.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Right, I get it.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

That's the analogy here.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay Jeremy.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Great, great discussion. So I think we've covered both basic and granular choice; we can advance the slide. So these first couple of critical actions are going to be covered by the Privacy & Security Workgroup; in general, one of the things that we want to encourage is that harmonization among the states regarding some of the statutes and regulations around the granular choice. And so while we're working on standards for basic choice, in the background, from a policy perspective, we want to see if we can simplify or help clarify some of the complexity around the more granular decisions. We can move on to the next slide.

And on this slide we have some of the things that we are asking the TSSWG to take a look at. And so you can see in that second bullet point in the 2015-2017 box, we want to know what technical standards we can put in the Standards Advisory to ensure that when an individual expresses basic choice, that expression is done in a standards-based way that is understood across the healthcare system. And so that's what we need your input on.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So Jeremy, this is Lisa. You're saying we need to capture it electronically and we need to do it in a standard way.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

And we can advance the slide. And so this slide also captures some more of the actions that are cover...that will be covered by the Privacy & Security Workgroup around the relationship of state government law to some of the more national federal laws. We can advance the slide.

And this slide captures the technical standards for basic choice. This falls within the wheelhouse of the Transport & Security Workgroup, because again, we want to identify the appropriate developers and stakeholders and to really harmonize those technical standards and the implementation guidance for consistently capturing, communicating and processing that basic choice across the ecosystem. And then in years 2018 and onward, that's when we want to start looking at the more granular choice; and you can see in those years we do have some critical actions around capturing the individual choice and capturing the more granular choice of what individuals express. So being able to say, share my normal health data, but not my behavioral records, for instance. And we can advance the slide.

And lastly in this category, there are some points around data provenance and so specifically harmonizing the technical standards and implementation guidance for associating individual choice with data provenance. So this is bringing in some of those provenance conversations we had at the beginning. And so this is also something else that we would like the input from the TSSWG.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Umm, Jeremy and maybe Julie can help out with this question, this is Lisa again. The task force that we did on data provenance in January gave recommendations for work that the S&I Framework initiative on data provenance is doing; is that work reflected in here or are we taking it a step further. I think you're saying carry the data provenance...in the data provenance data, include information about choice or sharing preferences or associating choice with data provenance to support choice. I'm trying to parse the wording there.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yeah, Julie, you're a little closer to the data provenance work, do you want to field that one?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right, sure. So Lisa, to your question, we included data provenance in this section so that we are able to say, is it generated from "X" source, right? So, at a high level that is how data provenance is reflected here. The work of the initiative, it's very early in the stages so it is not incorporated in here at all.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

And so Julie, this is the data provenance of knowing where the basic choice is captured, correct?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah and it's source...

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

So it isn't necessarily the provenance of the clinical data, this is the provenance of who captured that basic choice and documented it.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Hey Lisa?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

This is Jeff; I've followed the provenance and made some suggestions on the earlier discussion that we had and as I've seen to date, there's nothing in there at this time about concerning into a mobile device, so it stops at the level of an EHR traffic. So down even to the 11073 there is a gap. Now if that's changed, please tell me, but there's, from what I can see, from the sensor or from the device all the way up to the EHR, there is no data provenance in the S&I Framework to date.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

You know, I think that's something we're going to need to look at because...

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Okay.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

...I know that they are looking at providing provenance on the source of the data that's entered into the EHR, if that's...

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Yeah, but they don't really know...let's say you have a pulse oximeter that's made by some "X" and it's talking 11073 standard up to the phone. The 11073 actually has provenance in it but once you hit that spot, it is lost until it gets...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

...up to that, so that's a gap that I see...talk about.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Okay.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Okay.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I think my question for Julie again is, help me understand the connection between choice and provenance data. You just want to know where the proven...where the choice data originated?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Lisa, this is Lucia, I can probably answer that best for you because it comes...here's the dialogue, the behind the scenes dialogue about all that. We have this very complex environment that changes by geography, we just talked about that ad nauseam. There are sort of two ways to skin that cat; one would be simplifying the environment. The other would be to document the environment so that you ensure that your data uses were consistent with the environment where it originated, if that was required.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Does that make sense? That's why geography could be relevant to provenance. That's an argument, for example, that Micky Tripathi has talked about in other workgroups.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

So I'm not...you guys can...this is Lucia; you can tell what cat I want to try to skin first because it's harder and easier, it has probably better long term side effects to simplify. But, we may fail, we may succeed; we don't know, right? So that's why provenance becomes relevant and also it's relevant to things like a rule that's geographically...that manifests in a building; so part 2 manifests in building a place where...a location where federally funded substance abuse services are offered.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

So it's very physically specific, those rules. And that's not the only one like that, but it's the one most people are familiar with.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. And...can...are we also to deal with whether we think these actions are realistic within the time period in which they're listed?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Jeremy, I think that's fair game, don't you?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes, absolutely, that's...if you...actually, if you advance the slides one, so yes, you've seen this slide before; this is our general question. And so you can see in the general questions, those are things that we want to hear about...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Right.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

...is, are we including the right actors, the right stakeholders? Is the timing appropriate? Are we being too aggressive or could we be more aggressive? Are there any gaps? Are we missing any actions? Those are, in general, we want to have that feedback across all of the sections, in addition to the specific charges and questions targeted for each of the sections.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. That helps with that question. And Jeremy, are you at a place where you wanted to entertain additional questions from the members?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yes, that's all the material that I had for today. I have the general questions here and then on the next slide I had the summary of the specific questions, if you wanted to revisit those. But yes, that's all that I had to present today.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so what I'd like to do next is have the workgroup sort of discuss their reactions and any questions or concerns that you have about the task that we have at hand for the next two months. Thoughts, comments, questions?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEI Systems

So Lisa, this is Jason Taule; I guess the question is, in what format and what forum would you like us to undertake that effort?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So Jeremy, can you put up the slide that has the work plan on it, I guess it's the next slide, if you repeated it...no, maybe it's a previous slide, where we have the schedule of meetings and the timing of the work plan.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Yeah, I believe that's slide number 3, Michelle.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. So if you all can see that slide, and our workgroup is at the bottom, Transport & Security Standards, so today, at today's meeting we've got an overview of the roadmap and we've had ability to interact with ONC folks who could answer our questions in terms of the roadmap and the scope of our work.

We have until probably the first or second week of April to finish our task. At our next meeting on February 24, we will start having facilitated discussion that will enable us to generate draft or straw man

recommendations to each question that they ask. We will continue that process March 11 and perhaps the last meeting in March, which is the 20-something of March; at that point we should be finalizing the wording of our recommendation. Dixie and I will work with Julie, Michelle and Jeremy on the format of our recommendations, and perhaps it would be a good idea, Julie, for us to have that sort of worked out before our next meeting on February 24, so everyone can envision what we're aiming at, as far as recommendations. So I think that's a really good question; yeah, we have the scope and we have the questions you're asking us, so in what format would you like them and what should we be aiming at.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

So perhaps if we get them a few days before February 24, I think that the challenge is...the opportunity is great but so too is the work and I think three or four meetings may not be sufficient alone, we may need to put some time in prior to our coming together.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right, I think that's right. And Julie, that's, I think...Julie and Jeremy, I think that's going to be really important here. We had this with the task force on data provenance that I chaired in January, we really found that we had to do work in between meetings and we need to do everything we can to enable the workgroup members to be able to do that. So here we're asking for some clarification or guidance on the format of our recommendations and if we could get those sooner as opposed to later, that would help everyone think through what they can contribute at the February 24 meeting.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Lisa, this is Michelle. So I just want to share what we decided to do in two of the other workgroups that we had earlier today. So we have put together a template based upon the section that those groups were assigned and are asking all the members to provide their feedback on the questions that we're asking. For this group, though, perhaps it makes sense to divide and conquer and maybe there are different sections that we could assign people to so that we are able to have thoughtful reaction to all of the questions that are being asked.

So maybe we could plan for the next meeting to go through Section G, for example and assign specific people to walk through that with us. Just a thought on process, but just to make sure that the work gets done behind the scenes; ONC can certainly work to synthesize anything that members put together. But I think it's often easier to react to something than to do the work on the call itself.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, I think that's right and I think your idea of dividing up is a good one. Can we get some guidance on the format of the final recommendations that you all expect to see from all the groups? You know, when we did the task force last month, you guys gave a couple of examples of what you'd like the recommendations to look like or is there a specific format? What is it you're looking for and that can help us, too?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

So this really is comment and what we are hoping for is that the workgroup will come to consensus on what comments should be made. There may be circumstances, though, where the group doesn't come to agreement and we might want to share all of the feedback, so both sides of an argument, for example. Because it truly is just comments, not a recommendation; so, we can aggregate...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So do we...

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

...sorry, Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Do we do a presentation at the April 22 meeting?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Do we just submit the comments and summarize them at the meeting?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Yeah, I mean, we'll try to summarize them, make them...have them make sense, if you will. And somewhat similar to what a recommendation would be, but it's just a little bit different.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Thank you for that clarification, Michelle. So here...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Lisa, this is Lucia; I just want to one more thing. You guys obviously were asking for particular feedback for the workgroup and that does not deprive you of your right to comment as independent actors in your other capacities.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

So just remember, that whatever the workgroup hopefully reaches consensus on if you have additional thoughts in whatever other capacity you have in the rest of your life, this is public comment and you're allowed to make public comments.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right. So I, in fact Lucia, to use me as an example, I will be working in my role at HIMSS to help HIMSS develop comments and so many of you may participate in other efforts to create comments, and you can also submit them yourself through the public comment process.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Yup.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

That deadline would be April 6.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Exactly, thank you Lisa, you're a perfect guinea pig for that idea.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so to the person who asked the question about our work plan, I'm sorry, I can't recall who it was, does that discussion help you for now and then knowing that Dixie and I have a meeting with the ONC folks to do additional background planning. I will take an action to make sure that we get information out to you all soon, that allows you to be able to start to formulate input.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Yeah, this is Jason again; that's perfect, thanks Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay and we...you know, this is a dialogue so if what we send you doesn't help or you need something else, we can certainly be responsive to that. I think it is important for us, Dixie and I and the ONC folks, to provide everything we can to enable you to give us the benefit of your expertise and we don't want you to work hard on the process, we want you to have the time and the tools you need to actually give us your input. So, whatever we can do to enable that, we're committed to doing. Any other comments or questions?

I have a question for Michelle and Julie. Yesterday we had an email dialogue with Dixie and Dixie had a question about the presentation that Steve Posnack gave on the Standards Advisory document and it hasn't come up today because we don't apparently have an assignment relating to that document. Can you offer some clarification or guidance on that or even Jeremy, because I know you responded to

Dixie's email, but her comment was on the Standards Advisory document, so I haven't had an opportunity or a way to bring it up until now.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Lisa, this is Michelle, so in conversations with Steve, we decided that what we thought the best way to go about the Standards Advisory would be is that ONC would gather the public comment during this process, synthesize, aggregate the comments that we receive back and then share that with a task force that we form to talk about the Standards Advisory. So rather than having the Standards Committee workgroups look at it twice, we think we're going to have a consolidated effort when we're able to share the feedback that we received from the public with a group that is focused on it. Does that make sense?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So you...yes, so you are saying that the Standards Advisory document, while it was released at the same time is on a different schedule as far as the public comments, because I see that they're not due until the beginning of May, as well as the work of the federal advisory committees, that's all on a separate time schedule.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

It's definitely true that the advisory data has 90 days for response, right.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And then after that is when a federal advisory committee sub-body would get an assignment to work on it.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Yeah, likely in the summer months, if you figure May, then we'll need a little time to synthesize the comments and then we'll probably charge a task force with looking at it, once we have that more informed feedback.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so Jeremy and Julie, if you could remind me when we have our planning meeting with Dixie to close the loop on that so that she understands that we on this workgroup are not tasked with that document at this time.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Certainly; and just to add to that, there are a couple of specific questions that we are asking around that, though, so like for example, the basic choice, we're specifically asking what standards around basic choice would be candidates for the...advisory.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right, but Dixie's comment on the Standards Advisory document's lack of listing security standards, that's sort of...that would go as comment to that document itself.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Correct. Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

All right. Okay. Any other questions or comments for me or for the ONC folks that are on the line? Okay so Michelle, I think our next step is to open up for public comments, unless you have anything else or Jeremy if you have anything else.

Public Comment

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Let's open up for public comment and then we can do a quick wrap up. Operator, can you please open the lines?

Lonnie Moore – Meetings Coordinator – Altarum Institute

If you are listening via your computer speakers, you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. If you are on the telephone and would like to make a public comment, please press *1 at this time.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

So while we wait for public comment, Lisa I just want to confirm, did we agree that it made sense to parse out some of the work and so for our next call there might be assignments made for people to take on things?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes, I think we should talk about that with Dixie at our planning meeting, which I think is tomorrow, isn't it?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

The next one is next Thursday.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Next Thursday, okay.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

So I think Jeremy that that should be done via email sooner. So, we can follow up offline.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Right. No, that sounds fine. I want to defer to Dixie, she's the Chair; I mean, I think it's a fine idea and then we would just need to talk through how to do that if we want input from the members as to what they'd prefer to work on, that sort of, what is our process. But it's fine with me, but I'm going to defer to Dixie on implementing that so that could be an answer for now, Michelle?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

I think that's perfect, thanks Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

And we have no public comment at this time. So thank you everyone. Thank you, Lisa, sorry.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

Bye everyone.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thanks everyone...