



**HIT Standards Committee  
Transport & Security Standards Workgroup  
Final Transcript  
May 6, 2015**

**Presentation**

**Operator**

All lines are now 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. Also as a reminder, if you are following along via the webinar and you share any public comment, we may share that public comment at the end of today's meeting. I will now take roll. Dixie Baker?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

I'm here.

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

Hi, Dixie. 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. Aaron Miri; he is not here. Boban Jose? Brian Freedman?

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

Here.

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

Hi, Brian. Jason Taule? Jeff Brandt? 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?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

He said he may be late, we got...

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

Okay.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...from him.

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

We'll look for him. And Scott Rea? 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. From ONC do we have Jeremy Maxwell? Did we get Julie or Johnathan Coleman from ONC?

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

Johnathan sent me a message saying he was going to be about 10 minutes late.

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

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**

And Julie's here, Michelle.

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

Hi, Julie.

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

And Michelle, this is Lucia, I'm sitting in today.

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

Oh great, thanks Lucia.

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

Uh huh.

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

Okay with that I'll turn it to you Dixie and Lisa.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, thank you all for dialing in; we really appreciate the time you put into this today as the...we're going to hopefully undertake examining the other two NPRM standards that were assigned to our workgroup. Lucia, I'd especially like to thank you for dialing in, we're glad you took the time to listen to our conversation and we appreciate it.

Okay, looking at the agenda; the first thing before I look at the agenda, I wanted to mention that yesterday I learned that ONC recently published a new Privacy and Security Guide. And I was wondering if we might get the ONC staff to send that link, the link to everybody on this workgroup so that they have...they can be sure to see it?

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

Yeah, we'd be happy to provide that.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

That's great, thank you. We appreciate it.

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

This is Lucia; I just have to make a joke; you all should follow me on Twitter and you would have gotten it about 35 times between the publication date on May 10 and now.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Right, that's why I don't follow Twitter, because 35 times...thank you. Thank you. Okay, the first comments...set of comments we're going to review are the kind of updates from our discussion on April 21 and then we'll move on to the two new standards. I wanted to start o...do this in a different order from what it's listed on the agenda; I want to start with the privacy and security applicability. And there

are no slides about this, that's why I decided to...I just wanted to update you on the comments that I introduced at the Standards Committee meeting that and to tell you, or yeah, suggest to you some changes in our recommendation.

The first was that we looked at the security applicability for the clinical module and it said that it had all of them were applicable except data integrity. And you'll recall that we had a conversation about how important data integrity is to clinical functions and we suggested to ourselves that perhaps this was an oversight on ONC's part. I brought that up at the Standards Committee meeting and Steve Posnack said that it was not an oversight, that they intentionally left out integrity because they didn't...because the data integrity criterion specifically relates to...and the standard, specifically relate to transmitted data and he said that the clinical criteria don't involve transmissions.

But I went away and I looked at the criteria more carefully and the clinical criteria do include at least two, you know, very obvious transactions; one is the technology must be able to receive and incorporate a new or updated laboratory order compendium. And the second one is to receive and incorporate a formulary and benefit file. And in addition to that, depending on the modules architecture, it...other of the clinical criteria may also involve transmissions. So I would like to proceed with our recommendation, but to reword it to say that this is...the reason is because we do see transmissions within the clinical criteria. Is that clear?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Sounds good.

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

Yeah Dixie, this is Lisa; that sounds right. Thank you.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. The second one that...at the, now I wasn't at this last meeting because I was travelling but the recommendation was that the design and performance section also be made applicable. And if you look at the criteria that are in that section, there's really only one that has security implications and that's the application access to the common clinical data set, which I would agree has security applications...applicability, but I don't think...but the rest of the criteria are design attributes, not functional criteria.

So questioned that recommendation and I would like to suggest that we say that overall we agree, but the only exception is this application access to common clinical data set. And even there I wouldn't recommend all of the criteria; I think that we should recommend authentication, access control and authorization, auditable events and integrity only. So, that's...that as well.

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

Dixie, this is Lisa; that sounds right to me also.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, anyone else have any...okay. I didn't want to make those changes without explaining to you the reasoning that went behind them. Okay, the next thing on our agenda is...let's go to the next slide then. Go to the next slide, please. See, we only have two more left...two new ones, data segmentation for

privacy and eSMD and today we're going to also review our...the recommendations that came out of the April 21 meeting on C-CDA and auditable events and tamper-resistance. Okay next slide, please. Okay. Next slide. Okay and we've already gone over the privacy and security applicability and as you'll see, there are no slides on that topic.

So next slide; it should be on C-CDA...oh, this is just...this is a reminder of the method and metrics that the Health Information Technology Standards Committee uses to evaluate the readiness of a standard to become a national standard, of a technology specification to become a national standard. And these metrics were developed a couple of years ago and by the NwHIN Power Team and have been used by the Standards Committee ever since. You often hear John Halamka talk about them as Dixie's criteria because I was the author of the JAMIA article that was published conveying these criteria.

But there are two matrices, two major matrices; the Y-axis is the maturity of the...and this involves both the maturity of the specification itself and the maturity of the underlying technology. And finally market adoption, which we find is often a stickler with a lot of these specifications, that they really have not been widely adopted. Some of them are quite mature in terms of how long they've been RFCs for example, but they really are not widely adopted.

And then on the X-axis, we have adoptability which includes ease of implementation and deployment, ease of operations and intellectual property considerations. Ease of operations has to do with how much coordination that's involved in actually using the standard. Okay, and so as we proceed with these, all of these today's discussion, I thin...we always need to keep these two major criteria in mind, the maturity criteria and the adoptability criteria. And for those of you who've actually looked up the article, which is...there's a link there, you'll see that there's a lot of detail about the specific metrics to be used for each of these. Next slide, please.

Okay, this has to do with the Consolidated CDA and the ONC seeks comment on the maturity and appropriateness of the HL7 implementation guide for the tagging of health information with provenance metadata in connection with the Consolidated CDA. And secondly they are seeking comment on the usefulness of the HL7 implementation guide on provenance in connection with the certification criteria, specifically the...for transitions of care and view, download and transmit.

Secondly is the data provenance implementation guide maturity that the HL7 provenance implementation guide may be useful in identifying the origin of multiple sources of information but the questions, these are questions that came out of the last discussion, what about market adoption and adoptability criteria? Next slide, please.

Oh, I thought we had another one; I'm sorry, go back one. So, well, let me see...don't we have a slide that has look into the maturity of HL7 or is that it? Do we have another slide about data provenance?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Dixie, this is John Hummel. We were going to do one, but in your correspondence earlier this week, it appeared like we had contrary views so I thought we'd do discussion rather than a slide.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Oh. Okay, on data provenance?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District  
Yeah, because you had pointed out some things that I thought were pretty good in terms of the maturity of the underlying technology, the HL7 seems to be mature, but not very many people are using the data provenance technology in the current HL7 feeds.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah. Umm, the...I'm not sure that that was my comment but actually I did check with several people who...vendors actually, to see how broadly this provenance...let me back up a bit. I thought from the last...my understanding, having not been there, that from the last meeting two things was one is consider the provenance task work that Lisa Gallagher's group did in January that was reported at the January Standards Committee meeting and was not mentioned in the NPRM. And secondly, I was going to do kind of an environmental scan to see how much this implementation guide, how widely it had been implanted. Is that right?

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

That's right.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Yeah.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. So let's start with Lisa, to get feedback relative to how consistent the NPRM is with the recommendations of the task group that was convened in January.

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

Well the task group had to do with the scope and focus of the S&I Framework Initiative use case.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um, hmm.

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

So it's not exactly 100% aligned with the question that ONC is making here, but knowing the timing, I thought that we should refer them to that...to our recommendations so that they have that in consideration, we're looking at data provenance in total, if that makes sense.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. Yes, so you're saying that in our response to the ONC, we should mention that they should look at, and give them a specific reference to that work that was reported in January to make sure they're aligned.

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

Correct.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. So...

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

So then their questions for us, because they didn't even consider the work we did in January, they're questions were primarily focused around the maturity of the HL7 initiative.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hmm.

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

It didn't really...they didn't have any questions for us on the use case or any scoping or anything like that.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay.

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

So that's why we ended up with two comments; one is...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay.

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

...hey, look at this work we did and two has to do with our response related to the HL7 implementation guide.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, okay. And these slides don't include those recommendations, but...okay. So the second part is how widely it's used based on not only what I knew beforehand and also what I heard from individuals whom I queried about this is that this implementation guide is not, has not been widely used at all. And some even question whether it actually is going to capture the kind of provenance data that physicians actually need to make decisions. Are there any...

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

So Dixie, this is Lisa. I mean I think during the time that we worked on this in January, we spent quite a bit of time talking about what the scope and nature of the provenance information should be and we placed recommendations in there which the Standards Committee adopted and forwarded.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hmm.

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

Now it seems reasonable to me that HL7 may not have that recommendation yet and I don't know whether or not the implementation guide can be adapted to follow that, but it seems like we need to push out the recommendations from the task force so that they're widely known. If you have someone making an implementation guide that really doesn't have that information, I would think we need an assessment as to whether they can migrate to that. We also need an assessment; quite frankly, from the industry as to whether we got it right.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

You know, we had some notional ideas in there that we put forward, which the Standards Committee accepted, but I think there's work to do and is that the right scope? Are those the right parameters to pass? And then it goes forward into an implementation guide, if that makes sense.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, that makes complete sense. So what we're saying is that it's not widely adopted and secondly it's not sufficiently mature because it really hasn't been aligned with the work of the task force or...nor has it really been...well, I don't know what...I think it was balloted with the DSTU one, I think, right?

**M**

Yes...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Lisa and Dixie, this is Johnathan Coleman, I just wanted to let you know that I was on the...I am on the line, I apologize for...

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

Oh good.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Oh good.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

...joining you late, but if you have specific questions for me or you'd like me to comment, just let me know.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah. Okay, okay. Yeah, wasn't...

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

I have a question for Johnathan.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, you're just in...

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

Johnathan, do you know the status of the relationship between the recommendations we made in January and the implementation guide?

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yes, absolutely. So the recommendations that were made in January from the Data Provenance Task Force were aimed at the work that was going on in the Data Provenance S&I Initiative and this particular IG that I think the workgroup is looking to comment on is an artifact that came out of HL7. Now the Data Provenance Initiative did closely support and work with HL7 in the development of the HL7 specification and so at the time of the first ballot, we did not have the benefit of the input and feedback from the task force.

However, during the ballot reconciliation activities, because there were a number of comments on the HL7 ballot, by the time that the CBCC Workgroup in HL7 with structured docs and the security workgroup were able to get resolution on all of the ballots, we did have the input from the task force. So they have been factored into the latest reconciled version of the DSTU, Data Provenance DSTU at HL7. So hopefully that answers that question, I'm sorry if it was long-winded.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

So they've been factored into DSTU 2, right? Not 1 because 1 was balloted in September.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yeah. Yeah, well technically it'll still be the DSTU because the one that was in September was the ballot document and...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

...then as it's been reconciled, it will be published as the first DSTU, so that publication is going on right now.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Oh, I see. I see, okay. Okay.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

And then as far as the maturity, Dixie your comments really resonated very well with me about adoption and utilization. And the original project scope statement for the HL7 Data Provenance Project was put forward to HL7 last year to recognize the fact that there are existing, widely adopted standards such as the CDA itself...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hmm.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

...that contain information about data provenance, but it's very difficult to find them and to understand them and to use them. And so the point of the HL7 IG, which is just a, I guess, a small part and distinct from the overall S&I Initiative. But the HL7 IG was designed to take those existing specifications and harmonize the data provenance conformance statements across those specs so that there is a single go-to place so if somebody wanted to implement data provenance consistently with an IG, they had one place to go and look for it rather than having to tear through 8 different HL7 specs to find that information.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

That's real...that's very, very useful, Johnathan; thank you very much. Yeah.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Thank you.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

So the purpose of that whole activity was to draw out the provenance attributes as provenance attributes so it's ready for industry adoption, but it certainly isn't widely adopted.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Right. Consider it an overlay, or like a new overlay that takes what's already out there and constrains it and makes it more readily implementable in a more uniform way.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

I think that was the goal.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Now are those attributes primarily this is where the data came from or this is how the data were generated? Like I know a lot of...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

So this is...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...clinicians are very sensitive, for example...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yeah.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...to whether it was, you know, the data were generated...were actually entered by a physician versus NL...derived from natural language processing.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yeah, you've absolutely nailed the crux of our deliberations within the S&I Initiative and within HL7. So the end use case that we're hoping to end up with is that if an EHR system is presenting information, let's say it came from a Fitbit and there is also information from an FDA approved pacemaker; then the physician may want to choose the information that came from the pacemaker.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hm...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Both may be valid, both may have been accepted and trusted by the EHR and they both may have come in through a variety of different means, whether it be a home monitoring device or a PHR. So the whole point is to allow the clinician to make an informed decision about which piece of data that they want to accept moving forward.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, good, good. Okay. Okay, so discussion from those of you out there. So at the last...so the last meeting the outcome was that we were going to have this discussion, is that correct? Lisa...

**M**

Yes.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...you chaired that meeting that was right?

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

Yes, that's correct.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, so let's have some discussion on what you've heard today.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

This is John Hummel. I think that the kind of putting them out on the overlay, as it was stated, to make it into a...or clearer statement of what we're trying to do with it in terms of the requirement. But I would also agree that the use of the provenance is not very widely done, although I think that the technology the HL7 is mature enough to try to use it and it be my recommendation that we moved forward with the recommendation to the ONC to go ahead and try to use the HL7 IG for that purpose.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well to try to use is not what you put in a regulation; try to use means that we should...that means we should say yeah, it looks like this is going in the right direction, ONC should support it's further use and piloting. You don't...just because it sounds like its good is not sufficient reason to say it should become the national standard because keep in mind, if we...if it's in the regulation as the national standard for certification, then every single product, every single vendor has to imp...that is implementing these data provenance for their certification have to use that standard.

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

This is Steven Lane, can I just ask either John, you mentioned that it's being used by some folks; does anyone on the call have any experience with this where they've actually seen it in use and seen how its worked and can say anything about how functional it has been?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

This is John Hummel; I can say commercially I have not seen this available in any of the products I'm currently using. Just on some of the HL7 work I've done in the past I've seen the programming for it, but I've not seen it actually put into an application.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

And none of the vendors that I asked have implemented it.

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

So I mean I'm with you Dixie, I think it's probably a little premature to say this is a national standard when even people on this call haven't really seen it in use. Is there any way that we can encourage the testing and adoption of this, you know, in anticipation of or in support of it potentially becoming a national standard?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, would the slide driver go back to the graphic? I want to show you what that graphic is saying about exactly this topic. Is anybody driving the slides? Back, there, there. See, only the very, very widely adopted...very, very widely adoptable and very mature become national standards, up there in the upper right hand side. Those that we think, yeah, this looks pretty good and we want to suggest that ONC support their further development and piloting and use are in that pilots band, right? Emerging standards are sort of, somebody wrote it up and thought it sounded good but really very few people, you know, it hasn't existed very long, very few people have tried to use it, those are really immature.

But I think that this one does fall into that band for piloting fairly well because especially what Johnathan was pointing out, it grew out of the existing C-CDA implementation guide and it's kind of an overlay to it, so it should be useable, but it really has not been used. So it is in that stage of saying nice things about it, but recommending give it more time and support its piloting.

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

That sounds like where we want to be then.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Yeah.

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

Yeah, I'd agree...Brian; that makes a lot of sense, too is that you have to have more pilots to basically prove that it actually works.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, that's exactly what that's intended to be. Okay, okay. So we'll encourage ONC to support further piloting and we'll commen...in our recommendation we'll commend the work that led to it and say it's an important thing, but that we need to...we want to encourage support for more piloting and use...implementations.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Dixie, this is John Hummel again. I'd say that two is that if we can promote this as a way of getting more trusted data through the provenance, I think it would make the interoperability that they're trying to achieve a lot better because they're using trusted data.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah...that's good, yeah.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

So, I'd agree with...yeah.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes, yeah, I totally agree. It's...and of course that's why it was assigned to this workgroup is that provenance has so much to do with data integrity, you know, how much you can trust the data. So we will, once again, say how important it is to data quality and integrity. Okay.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Good.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

That's a good point, thank you. Okay, let's get back to where we were and go to the next topic; so thank you. Fast forward the slides about...to where we were, please. Let's see, is this the first slide about auditing? Go to the previous...let's see...auditable events and tamper-resistance. Umm, okay, so this is the first slide on auditable events and tamper-resistance. The question was should ONC explicitly modify, add to the auditing standard to require change of privileges to be audited or is this already audited at the point of authentication?

First of all I want to point out that certification doesn't require that anything be audited; the certification requires that things be auditable, but the question is, I think, is should we explicitly say that changes to privileges be auditable? So look at the next slide, please...go to the next slide; meanwhile, I'll talk. Maybe...

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

Next slide, please.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...pardon?

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

This is Lisa; I was just reminding them next slide, please.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah. Maybe if they just hand it over to one of us it would be better. But, I wanted to bring up that...give you a little of history. This...the Security working group has...thank you...has been asked a number of times to comment on what events should be audited...auditable and Lisa and I kind of always go, why do they keep asking us this question?

Now what's in the certification criteria today, the standard that's in the certification criteria today is ASTM E4127-01, which is auditing and accounting of disclosures for healthcare; that's what that standard is all about. And so section 5 of...section 7 of the standard specify very clearly the data elements that need to be collected per event. And section 5 says that the audit log is a record of actions, queries, views, actions, deletions, changes performed on data by users.

But nowhere in that standard does it outrightly say, and nowhere in the regulation does it outrightly say that the technology must provide the ability to record information about security relevant events, which is what an audit is for. A security audit, the purpose of a security audit is to collect information about security relevant events like creating an account, deleting an account, changing privileges, the question that we were just asked, the, you know, change of a password; all of those kind of things are recorded in the audit trail. So there we...there's a need, a serious need, for there to be a criterion in the regulation that says, that requires that the full range of security relevant events be auditable.

Unfortunately, this ASTM E4127 doesn't do that, nor frankly does NIST 800-53 R4 do that. And so we're looking for your input on what kind of a thing should we just state, make a recommendation that it says that the module must be capable of recording information required by 4127 regarding all security relevant events? Should we list them? Do we have an example that we can pull from? What do you suggest we do here? But this is why we keep getting these questions. Now it's like the light bulb went off, we keep getting these questions because 4127 doesn't address it.

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

So Dixie, this is Steven Lane; I mean, I can't point you to a standard but I think the idea that these events as outlined on the slide should be auditable makes perfect sense. You were saying a couple of minutes ago, whether it should be a standard that they are audited, and I think that's harder for us to say, but I think to say that they should be auditable makes sense as a standard.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, typically the, although some questions we get from ONC suggest otherwise, but typically when you do a certification of any technology, whether it be healthcare or an operating system or anything, you're testing on the capability to do something, you're not imposing policy.

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

Yeah, that makes sense.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

I just thought I heard you say the other earlier.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

I pro...I might have, but I meant to say auditable, not audited. Yes. I think the...oh, I know, the last slide, that was how the ONC phrased it, they phrased it as audited, but I think they meant auditable. So are there...do others of you know of standards. Another standard that was mentioned to me was ATNA, IHE ATNA standard, which also, just like 4127, only addresses the auditing of events related to opening a record and reading the record and changing the record; it doesn't include all security relevant events.

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

This is Brian. I wonder if, because I think if we just...if we gave an overarching kind of thing that says, you have to have auditable events, security auditable events, somebody could come back and say, well, we don't consider this a security auditable event or something.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes, exactly, yeah, that's the risk of that, yeah.

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

But I think listing them, too; there could be some missed so...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Exactly. Yeah, that's why I wouldn't, I really don't want us to make it up, but if we had some, you know, acknowledged...knowledgeable source, it would be...even if it weren't a standard, if we borrowed from it, it would be better. Ideally it would be nice to have a standard that listed the auditable events like this, you know, like the operating system standard of years ago used to list security auditable events. Lee Jones, you're on here, do...you've been around a long time on this sort of thing, do you have anything to suggest? I heard him come in.

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

Yeah, I'm here.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah. Do you know...I know you've been around standards a long, long time; you probably worked on ATNA, in fact...something we could...

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

Yeah, I mean I think that...I guess my practical side is that there's always a debate about what an auditable event is; I mean using the standard, ATNA, certainly things that I've seen cited in places and put into contracts and that we had to comply with ourselves in different times, it just always is a debate

about what kinds of things should go in there, because obviously there's a lot that can be written down. So...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well ATNA actually us...cites 4127, but both of them are restricted to security relevant events related to the electronic health record. And I think we're looking for something that is more comprehensive. Maybe we cite, Brian, back to you, the security relevant events, but we include an e.g. list, you know, like this.

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

And I wonder if...I could do a little bit more research for you, because I wonder if there's something in PCI or something embedded in one of the NIST standards, I guess.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, I thought I'd see it in the FISMA, you know, the 800-53 R4, you know, FISMA, wouldn't you think it would say exactly what events need to be auditable, but it doesn't. It says you have to identify those events that your organization is going to audit. I think that that's probably because it's related to an organization rather than specific technology. But PCI might be useful, that would be great, if you could do some checking for us, it would be...and maybe make a recommendation on what we might put...suggest.

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

Yeah, I mean I think that's what...Lee Jones again, what I was saying is that it seemed, in my experience, it's just a statement by vendors about what the audit, there's no definitive list of auditable events. I mean there are some that there is wide agreement on, but then theirs may not be comprehensive.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

If you said...if you gave a vendor security relevant events must be auditable, how do you, because I've...this has come back to us a number of times. Then they come back and they go, how do you test for that? If they come out and they say, well we are able to audit somebody opening a...accessing a database, but they didn't audit somebody logging on or creating an account or attempting to log into the system an excessive number of times; you know, all of those kinds of things. I don't think, could you...well, it's a question really. Could you then deny them their certification because they didn't audit all security relevant events?

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

And is this just security relevant events on a federal level, because states like we do work in certain states that impose their own regulations around how you do certain kinds of things with certain data. And does that now get grafted into this? It seems not if you're talking about a national certification, but it just goes to underscore this idea of what is an auditable event in this context is in the eye of the beholder.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Yeah, the California law that requires clinical history to be now to be able to be audited for any changes and what was the prior state prior to the change and then who made the change, I think, is a good example of that.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

That is a r...yeah, that's a good example. Yeah.

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

This is Brian again, but Dixie, I can do that and...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. We'd really appreciate that if you just look around and see what you have. I think you have a good grasp on what we're looking for...something you can hand to a vendor and say, build a system that does this.

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

Right.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, thank you so much. Okay, I think we have another question they ask us, would you next slide, please. See this is this is where it steps over from auditable to audited. They ask whether a critical subset of events should be enabled at all times. Currently audit logs can be disabled and...but you have to identify when, by whom, you know; you have to audit that it's disabled. So, ONC has asked us these same questions before, but they're asking again, is there a critical subset of auditable events that should never be disabled, which means you make them audited versus auditable. Is there any alternative approach ONC could or should consider? And what are any negative consequences of keeping a subset of audit log functionality enabled at all times.

Now we di...as it says here, we did, the workgroup in April of 2014 answered this exact question, I think that's on the next slide, right? Next slide, please. Umm, this was our...is this what we put in for...no, this is the straw comment. Is the next slide, I should just bring it up so that I can see...okay, this...is it in the appendix where you have the recommendation from before?

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

Dixie, I'm going to look, I have it up so hold on. Yeah...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

...it should be in the slides. Umm...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Last year the April recommendations, the standards group said that...

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

Yes, on slide 24.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Ah, good. Excellent. Okay, could we go to slide 24; thank you so much. Sorry for all this skipping around here.

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

Yeah again, here they're ans...asking us a question we've already answered so we wanted to make sure that we had our own history here before we made any decisions.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes. So here's what we said in April, 2014. It says, I have a very small laptop...although the current certification criteria doesn't preclude the audit trail from being disabled; in other words we were saying what this group said is that it's up to the organization. They do require access controls restricting the capability to disable the audit log to a limited use of identified users. So, we're saying...we were saying that generally an organization will only assign one or two people to manage the audit trail, because it is so sensitive.

And the bottom line there, you can read it as easily as I can, but the bottom line was that while the Privacy & Security Workgroup doesn't suggest a regular practice of disabling the audit trail to manage storage, it does suggest that certification criteria should not thwart administrative ability to perform the assigned functions. What they were saying is, in an emergency, and one of you mentioned...alluded to this a while ago; in an emergency sometimes an audit trail, which takes a lot of storage, is the number of events that are audited is reduced to save storage. In an emergency, you really can't even anticipate what's going to be the impact.

So at least that working group suggested that no...nothing should be mandated in the certification criteria to always be on. So, as Lisa said, that gives you the history of what was recommended before. Now we can go back to the slide that we were on, please. Okay; so, discussion on that?

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

I...this is Lee Jones; I agree with that you shouldn't force the organization; they can determine their own risk tolerance and...factors that the makers of these regulations can't necessarily anticipate.

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

This is Lisa; I agree. We continually hear from the industry that they need some administrative control of this and it's...for storage, maintenance, disaster recovery, other things and so I think we reviewed this the last time and I don't see that anything has changed. And I think our recommendation from last time was thorough so that when there's an audit of the events that disables the audit log and those controls around it should be in place, again as we said, based on risk but I think we go with no change to our recommendation.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay.

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

This is Steven Lane; I agree.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. I do like the...let's make sure that...I like what...that Lee tracked it back to it is a risk management decision; so let's make sure that our response refers to a risk management decision because that's in a nutshell; it's always a risk...

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

Totally agree, thanks Dixie for catching that.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay; that's what we'll do. Okay, next slide. Now, getting into the two new topics; data segmentation for privacy and electronic submission of medical documentation. Okay, DS4P first; next slide, please. ONC to...proposes to adopt two new certification criteria that would focus on the capability to separately track or segment out sensitive health information, the data segmentation for privacy sending and data segmentation for privacy receiving. Next slide, please.

Okay, here is what the NPRM says, the technology must enable a user to create a summary record formatted in accordance with each of the standards adopted in 205(a)(3) and (4) that is tagged as restricted and subject to restrictions on redisclosure according to the standard adopted in §170.205(o)(1). Now, §170.205(a)(3) and (4), those are the data segmentation for privacy, right? What's the (o)(1)? Is my MITRE...is my ONC team there to...okay. It would be useful to know...

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

We're looking it up. If I recall correctly, the (a)(3) and (4) is the CCD standard and then (o)(1) is the data provenance...or the data segmentation for privacy standard.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Data segmentation for privacy send and receive is a single criterion?

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

No, so there's one criteria for send and there's one criteria for receive; so this is the send. So the 205(a)(3)...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Oh, I see.

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

...and (4), I believe that's referring to the document...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hmm.

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

...the summary record formatted in accordance with the standards adopted in 205 (a) (3) and (4) I think that's C-CDA. And...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, good, good, that's very useful; thank you.

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

And then 205 (o)(1) is the data...the reference to the data segmentation for privacy standard.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Send...yeah, I know...

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

We're looking that up, give us a second just to confirm that, but I believe that's what those references are.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, I didn't notice that this...yeah, this slide is just send only, so we're talking about data segmentation for privacy and you have to be able to tag a C-CDA in accordance with DS4P. The next slide I think probably addresses send...or receive. So next slide, please; data segmentation for privacy, receive, must enable a user to receive a summary record that is tagged as restricted and subject to restrictions on...in accordance with DS4P. And (1) must be send and receive. And so the...so, it's one standard, they're referring to the standard, it's a single standard DS4P, but there are two different certification criteria that both point to that same standard.

So they are proposing to require document level tagging and sequestration of the document from other documents received. And view the restricted document or data without incorporating the document or data. Now the criteria you see here came...were derived directly from recommendations that came out of the Privacy & Security Tiger Team, which looked at...which is in the policy side of the house; it's a Policy Committee...it was the Tiger Team and now it's called the Privacy and Security Working Group of the Policy Committee.

But they came up with the recommendation that in order to really enforce what SAMSHA regulation requires for behavioral health, and that's really what DS4P is all about, for behavioral health you need to be able to receive that restricted document, but in order to really continue to protect that data against secondary release, which is also in the SAMHSA regulation, you need to sequester the document rather than splitting it up and putting in different fields in the EHR. So that's what they're talking about here.

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

Dixie, this is Lisa; I have a question and maybe Jeremy can answer it but, what exactly does §170 (o)(1) say? I mean, what is that standard that it's referring to and what exactly does it say? Because I looking in the backup slides and I don't see anything there that helps me understand it, §170.205 (o)(1)?

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

Yeah, I just pulled it...

**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**

Yeah, I just pulled it up in the NPRM public instruction copy and so it's the HL7 implementation guide, data segmentation for privacy release 1.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

So were...are we being asked about the sufficiency of that standard or...just like we were the previous HL7 implementation guide or are we being asked a different question?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

No, our whole question is about whether it should be a standard in 2015...certification criteria standard in 2015, so that's...

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

And then that would be...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...that's our...

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

...and that would be predicated on our evaluation of the maturity of that standard, right?

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

Correct.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

The maturity of the standard and the implementability of the standard.

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

Correct.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

So if we had anything to say about either of those, we...it's fair game; but we shouldn't be saying, well, I don't like the metadata tag that they recommended, you know, it should be its readiness to become a certification standard.

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

Right and I just, I don't...I think that's the conversation we need to have. I just don't have any background on the maturity of that standard at the present time.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well I do, a little bit. It is...because we've talked about it in other groups and in this group and in the Standards Committee and to my knowledge, nobody has implemented DS4P beyond the demonstration implementations in Connect-a-Thon. They...it has not been...in fact, it hasn't even been an HL7 standard for that long, but it has not been...pretty much at the same provenance.

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

Hey Dixie, there were a couple of sites that have implemented it, specifically for 42 CFR Part 2...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hmm.

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

...to address that use case. I know Prince Georges County and there may be...others. So we mentioned that in the preamble of the rule that there were a couple.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

And they've implemented it as pilots or as fully op, you know, fully operational?

**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. So Dixie, this is Julie. So the pilot that Jeremy just referenced is the one from SAMSHA and it was called the Consent to Share and they did do it as a live pilot and using live data; so, if that helps the group at all...right and it's pretty much being used now.

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

Um hmm.

**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**

One thing that we would note is that it is specific to 42 CFR Part 2 and the implementation of the DS4P standard within their consent to share open source tool is within the constraints of the workflow of that organization.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well actually the... Joy Pritts and her team used to always make this very, very clear that DS4P was specifically designed for Part 2 enforcement and in fact, what the Tiger Team policy is...was talking all about behavioral health Part 2 data. So really that's the only use case that DS4P was actually designed to enforce, because that's the only law out there right now that requires the kind of restriction on secondary distribution and use. So...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Hey Dixie...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...the fact that its Part 2 is not...shouldn't be a ding, that's really...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Dixie?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...um hmm.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yeah Dixie, you're right, this is Johnathan. Would it be okay if I made a quick comment on that please?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes, please yes.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Thank you so much. So I was the initiative coordinator charged by Joy Pritts and ONC in running that initiative and from the beginning, the standard was intended to be more broadly applicable than just Part 2, but recognizing the variance in state laws and the privacy techniques used internationally, the DS4P use case was exactly predicated on Part 2, but it was also intended to be extendible and used for other privacy policies that were perhaps less broadly applicable, like specific state laws. But also I think it's worth noting that Title 38 in the VA, which is not specifically behavioral health but also includes other conditions such as sickle cell anemia and HIV, was a driving factor in the development of the DS4P standard.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Great, thank you. You said it much, much better than I did, but thank you very much. Right.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Sure.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

I knew that they always developed it around DS4P as their use case, but I...I yeah, good, good. But it was designed to be used in other...for other...enforcement, it was primarily addressed at enforcement of law, you know, where it...well, it really wasn't designed where one organization kind of decides to segment out data. It's really designed...

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Right.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

...for exchanging data that legally is required to be separately recognized and separately protected.

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yeah, absolutely and in hindsight, maybe segmentation was a bad term for it because I think especially with the behavioral health implementations the idea was to get important information flowing more freely to those who are authorized to receive it. And having a degree of control about its potential reuse might empower providers to more readily share it to authorized receivers rather than say, you know what, this is so sensitive I'm just going to wait and send it manually.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, yeah.

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

I think that's a good point.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Hmm? Yeah, it was.

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

I think that's a good point Johnathan made; Dixie, this is Lisa. It's...even knowing that it's been piloted and assuming, I guess, we should assume that the pilots were successful and that it's been operationalized in those organizations that you Julie and Jeremy mentioned. I mean I think we need to seriously think about recommending this so that we have a pipeline on the products that have this capability. But I just, you know, right now the information on the pilots is anecdotal and maybe we want to be double-checking that. But, other than that I think maybe we consider moving this forward?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well the fact that it's been piloted does not make it...doesn't...isn't sufficient. That me...puts it in the piloted bracket, that doesn't put it into the ready to become a national standard bracket. You know,

what puts it in the national standard bracket is if it were...is if it had been adopted widely and piloting is not the same as broad adoption by any means.

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

Well how, I mean, I guess my question is, when we're being asked should these things be put into a certification standard, you know, that's the lever that makes it widely adopted, you know, so I don't...I think it's like almost a chicken and the egg thing. I mean, we know we have this policy requirement and we know that it could possibly be impeding the sharing of information under...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Um hmm.

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

...necessary circumstances; so how do we get it there if we can't put it in a certification requirement, how do we get it widely adopted?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well, Steve Posnack talked about that they do have other levers to encourage org...encourage vendors to implement ahead of time, you know, to encour...to give them a snapshot of what's coming down the pike; you know, he's often talked about that, how we really need to give them some idea of what is being considered, but that doesn't mean that it's ready to become a national standard. I would argue strongly this is not ready to become a national standard.

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

Because it's only been piloted, is that the reason?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes.

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

Or because you think there's something wrong with the standard?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

No, no, no, no criticism of the standard whatsoever.

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

Okay.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

That it has just been...I would say the same thing here as we said about the...about provenance, data provenance that it looks...it's an important standard, it addresses a very important problem, you know, is when you do have to...when you have state and federal law that forces you to segment out data and

treat them differently, certain types of data. It certainly addresses a very important problem, but it really has not been widely ado...hasn't been adopted, it's been piloted.

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

Well so then do we have...should we make a comment on both of these about how we think we can, you know, what is a path or what are potential levers...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

...because I think these need to be moved forward and so anything that we can think of that will help that, I think would be productive.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

I think so, too.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

I think it's a...suggestion yeah.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

I think so, too. I think ONC would appreciate hearing that kind of thing, not just it's not right...quite ready, but if we had specific actions that we thought they should encourage...do to encourage its adoption, we should mention them.

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

Okay, now we have to think of them.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

Johnathan, any thoughts on that?

**Johnathan Coleman, CISSP, CISM, CBRM, CRIS – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.**

Yes; no, it makes sense, I mean I agree with what you're saying and in general. I think that there may be more implementations out there than perhaps we're all aware of. I recall that there were some implementations in the Tampa Bay area as part of the Florida or Tampa Bay 2-1-1 referral network and I recall talking to some folks last year, in 2014 about the DS4P capabilities being included in the production systems in some of the larger...at least one of the large EHR vendor production systems; so not just a behavioral health, but the general EHR system. So I think maybe there is more up to date information out there that we might not have at our fingertips and it might be worth pulling that together before...concluding, perhaps.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, I agree.

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

I think so, too.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

But we'd be asking, I think knowing about other pilots would be interesting, but more importantly is who has stepped up and implemented it because they see a business need to implement it; that's really the point.

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

Yup.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Because to implement pilots because somebody paid you to implement it, you implement in production systems because there's a business ne...business driver for it. And I think that's really what the government gets dinged about all the time, you know, is when you impose standards where there's no business driver for it. And I think if we can show that there is a real business driver for this that people have stepped up and implemented it because of that business driver; that would be the argument we should look for.

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

So question to Jeremy; is there a way that we can see what the implementations are, sort of get some information on that?

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

Ah yeah, we were just on mute here at the ONC folks, figuring out a way that we can pull that list together. We'll work on it.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, that would be really useful, perfect. Thank you. Thank you and then we'll address this at our next meeting then. That would be great. Okay, I'm making myself a note. So, how are we doing for time, see this is...we're doing okay for time, aren't we; right? This goes to...

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

We have 20 minutes left.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, then let's go on to the next one. Umm, the final question that was...standard that was assigned to us is electronic submission of medical documentation or eSMD. Next slide, please. Okay, the NPRM proposes four basic capabilities; the capability 1 is to create...this is to create a document to send to CMS, I mean, we've had to give you some history. The eSMD has been...was presented to the Standards,

full Standards Committee about a year ago, I think and then subsequently there was a separate meeting with the eSMD folks from CMS. It was developed...eSMD was developed by and for CMS basically, through the S&I Framework process.

Then it was a separate meeting that it was presented to the clinical and security working groups. And what it's for is when a claim is submitted to CMS and it requires more documentation to back up that claim, they want to be able to ask an organization to send that additional documentation, and they want to make sure that they get non-repudiation and security around that submittal.

So, the capabilities are to create a document. Secondly to embed digital signatures in the C-CDA document; so the document comes across as a C-CDA and they want that there could be within the C-CDA document, individual sections that were from different departments, let's say, you know, from the...one from pharmacy or something, or from different physicians who saw a particular patient. It could be multiple creators of content in that single C-CDA, so they want to be able to embed these...each of those would be digitally signed.

And then to create this overall external digital signature so the manager of document control or whatever, whoever it is that's responded to CMS, is then signing the overall C-CDA as an entirety. And then finally, create and submit digital signatures that assure both data integrity and non-repudiation. The C-CDA specification calls for using the Worldwide Web Consortium cross something...digital signature standard. And that is just a...that's not the algorithm that's used, that's the packaging standard that packages it up using XML tagging and it specifies the XML tagging, etcetera. So, next slide, please.

So, when this, as I mentioned, eSMD was presented to the full standards working group in July and August of 2013, holy cow, it's like almost two years ago. The...and there were two things that were brought up when it was presented, two primary concerns; there was a lot of discussion, but two primary concerns that were brought up by the full Standards Committee. One that they were proposing to use a digital signature standard that was different from the DEA standard for electronic prescribing of controlled substances, which would require an organization to implement two entirely different digital signature mechanisms within their organization, and the Standards Committee felt that it should be consistent.

And second was perhaps even a larger concern was that the standard itself has a lot of workflow embedded in the standard, it's not strictly a technology standard by any means; it talks about this one sends this, you know, the whole workflow. So they were saying that it would require significant changes to existing administrative and clinical workflows to incorporate the specification. So, next slide.

Our ONC team looked into the specific algorithms that are used by eSMD and DEA and found that they use the same digital signature standard, which is DSS, but they use different revisions. And I don't think either one of them...yeah, right, looking at this, neither on...both of them were superseded by FIPS 186-4 so both of them use FIPS 186 and 180; I think 186 is RSA and 180 is SHA, you know, SHS...the hashing function and the...yeah, PKI, 186 is RSA PKI, that kind of thing and the 182 is the hashing function. And both of them were...have been superseded by 186-4; so, it's possible that both of them could be brought up to the same algorithm. And Jeremy is our resident encryption expert, so did I explain that? Is there anything you would like to add?

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

No, I think you captured it.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay.

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

Dixie, this is Lisa; I have a question for Jeremy, I guess. So we saw this briefing on the Standards Committee for...on eSMD almost 2 years ago; has there been any change to their standard, any update, you know, are they attempting to resolve the issues that we brought up when we first were briefed on this or is it just sort of the same as it was?

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

Yeah, we'll have to take a look at that, I'm not sure of the answer to that.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

I don't think there's any change to the workflow and I honestly don't think that this workgroup is the one to address the workflow...maybe, a couple of you certainly could though. But I think that...I think we certainly should check out to see whether the digital encryption standard has been, you know, what changes might have been made.

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

Yeah, I'm wondering too if this question was only given to us or if it was given to any of the other workgroups or even on the Policy Committee. I mean, at some point, you know, we...I think the Standards Committee was clear in its concerns around this and so if we get asked the same question again, I'm not really sure why. Like if nothing has changed, you know, what do they want to know from us? We can certainly tell them, you know, that there's been a new FIPS that they need to pay attention to, but I think the other challenges need to be addressed.

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

Yeah, hey Lisa, the...I can know for certain that the PSWG was not assigned the eSMD topic; I don't know about the other workgroups, though.

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

Well yeah, because if there are workflow challenges, it would be maybe other workgroups.

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

Michelle, do you know if this was assigned to any of the other workgroups?

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

No, it wasn't.

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

Okay.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well that's a really good...that's a very, very good point, Lisa.

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

Yeah, I mean I think we can't, you know, I think the Standards Committee's on record on this and so until this, you know, some of these challenges are addressed, we can answer the question that is within our scope, but it's pretty clear there needs to be some...a hard look at this situation.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, I think Lisa's really hit the nail on the head here. I think if we get Jeremy to check to see, check for us to see what changes might have been made in...since the Standards Committee and clinical and security workgroup were presented this and then report back, that would be helpful. But I think, you know, then I think we can figure out what parts of the previous comments that have been made might still be applicable and we could just include those with our response, but really focus on the security relevant pieces, which is the digital signature.

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

Yeah and I think my point is that we need to remind ONC that this issue hasn't been moved forward as the Standards Committee gave comments two years ago and we're being asked about the same standard. So either they, you know, the eSMD folks need to look at what they've got or, you know, what else can we say? You know, it's not moving; it's not going to work the way it is and so...

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah.

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

...I don't want to forget about the com...I think we remind about the comments that were made in 2013.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, yeah, that was a very, very animated discussion. Yeah, I think that's right. But...yeah. Jeremy, we would really appreciate you, and once again, this is a standard that...well, two things. This is a standard that is different from most standards because it does have so much workflow embedded in it. Most of the standards that we discuss really don't have that much workflow, I mean, contrast it with DS4P; DS4P really focuses on sending, receiving and tagging, you know, it doesn't dictate the whole workflow between organizations or anything like that.

So that...it's different in that way. Yeah, so...oh and secondly, it clearly hasn't been implemented, I don't think...I'm not ev...I don't even kno...I don't know about pilots or anything, they've probably done some pilots, but it hasn't been implemented by organizations. Does anybody else have any insights about eSMD? Thoughts? John, you're at a hospital...

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Yeah, I was going to say that the...I'm more familiar with the DEA; I'm very unfamiliar with eSMD.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Well do you know what, does DEA use the W3C standard for packaging the signature, although that's probably not really relevant. It's more transaction signature, right?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Yeah, it uses an RSA token to provide the extra layer of security.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, yeah. Do you know if they've updated to this latest versions of the FIPS standards to the version...?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

I don't off the top of my head but I could find out. We just went live with the DrFirst here at our hospital about 3 months ago and so in looking through the documentation that was provided then, it seemed like they were, but I'm not 100% sure.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yes, too bad Peter wasn't able to dial-in. He could probably tell us right away.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

Yeah.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, so why don't we table this one as well until we...pending getting...I think I should point out that in the materials that were distributed for this meeting, we included the...I think the minutes and the transcript, right? Is that right, Jeremy?

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

Yes.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Yeah, from those meetings, the standards, so you can certainly go in there and read about what was...about that conversation. Okay, are there...let's see, where are we? Do we have...I think that's...can you go to the next slide? Let me make sure. Yeah, we...the...at our...we have several action items here, let me go over those. We have, Brian is going to do some research on how we might suggest auditable events, or security relevant events to be auditable. And ONC is going to pull together a list of implementations of DS4P.

And Jeremy is going to check for us to see what changes were made, and of course we're talking about at a, we don't need like word for word. You know, at a high level what changes might have been made

to the eSMD since they presented it to the Standards Committee in August of 2013. Did anybody write down other actions from this? Okay, does anybody have thoughts that you didn't get out during the meeting thus far?

Okay, let me thank you again for taking the time to dial in and to participate in this discussion. Today's was really hard because it does have some topics here that are not as familiar to everybody as most of the topics that we're usually discussing. So, we really appreciate your participation and as you look through the materials that were distributed, if you have further thoughts, please feel free to share them with us.

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

And Dixie, sorry to interrupt, did you talk about the rescheduling of the May 19 meeting and why we were doing that or would you like me to?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Oh sure, that would be good. Yeah.

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

So our next scheduled meeting is May 19, but we would like to move that to next week for a couple of reasons. So the primary reason being that the Standards Committee where we have to present the NPRM recommendations is on May 20 and so that doesn't provide enough turn-around if we have our meeting on May 19 to review the final comments. So, especially given that we have a couple of the action items that we discussed today pending. We want to have one more meeting to...for you guys to have a chance to review and make sure that we have all of the language right around the recommendations before we go in front of the Standards Committee.

And additionally, some of the Chairs are travelling and things like that. So, from a scheduling standpoint, we are going to move the May 19 meeting to next week. We're still trying to lock down a date. Michelle, do you have an update there on, has a date been decided or do we still need to work through that?

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

I think we still need to work through that. Altarum is working on finding a date.

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

Okay, great. So we will work on getting updated invites out to you guys before the end of the week.

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

Not to make it...this is Brian; not to make it more confusing or hard, but I mean, not that it matters, just Wednesday May 13 just won't work for me, I'll be unable to call in. But, I could still send in any recommendations or things that I find before then.

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

Okay. Yeah, since it's out of cycle, we have to, you know, schedule it with the recognition that there are other working groups that were previously, you know, regularly scheduled for next week so we kind of have to work around them. But we'll try to take that into advisement.

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

Okay, thank you.

**M**

That's it?

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

Are we ready for public comment?

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay, thank you very much everybody and I think we're ready for public comment.

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

Caitlin, can you please open the lines?

**Public Comment**

**Caitlin Chastain – Junior Project Manager – 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 phone 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**

We have no public comment.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Okay. Thank you and thanks to everybody.

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

Thank you everyone.

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

Thank you.

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

Thanks everyone.

**Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates**

Bye, bye.

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

Thanks, bye, bye.

**Public Comment Received During the Meeting**

1. Good reference <http://healthcaresecprivacy.blogspot.com/2012/09/meaningful-use-stage-2-audit-logging.html>, from John Moehrke