



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
April 21, 2015**

Presentation

Operator

All lines are bridged.

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

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Policy...I'm sorry, 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 also state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Lisa Gallagher?

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

Here.

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

Hi, Lisa.

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

Hi.

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

Dixie Baker? Aaron Miri?

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Here.

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

Hi, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Hello.

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

Boban Jose? Brian Freedman?

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

Present.

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

Hi, Brian. If you...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, present.

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

Hi, Lee.

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

Hello.

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

Peter Kaufman? Scott Rea?

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

G'day, I'm here.

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

Hi, Scott. Sharon Terry? Steven Lane?

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

Here.

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

Hi, Steven. And from ONC do we have Julie Chua?

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

I'm here.

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

And Rose-Marie?

Rose-Marie Nsahlai – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I'm here.

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

I'm sorry. Thank you. And with that, I'll turn it over to Lisa.

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

Thank you, Michelle and wanted to say good afternoon and welcome to all the members of the workgroup and the members of the public for participating today. I appreciate everyone's ongoing support of our work. Next slide, please.

So today we are in the middle of our work stream to do comments on the Certification NPRM. So at our last meeting on April 8 we did some work on some areas that we're commenting on, and we'll do a brief review of that today. In continuing on our discussion, we will cover some new requirements that we're reviewing, C-CDA, data provenance and also auditable events and tamper-resistance, should time allow. And then finally, we will open it up for public comment; so that's our agenda for today; are there any questions? Okay, next slide please.

Okay, and this is just a picture or a table that we're using to follow our work plan. As I mentioned, we covered a number of areas at the April 8 meeting and our upcoming slides will cover a review of those, so, the overall health IT module certification requirements for the requirement area of privacy and security and then the specific requirements of automatic access time-out, end-user decryption...device encryption and integrity. So we'll go over what we determined our draft comments to be and come to finalization on those and then for today, we will proceed with the data provenance and auditable events and tamper-resistance discussion.

Just as a preview for next month's...our next meeting's discussion on May 6, we will be talking about data segmentation for privacy and electronic submission of medical documentation; and those will be our final requirement set for this NPRM. Our comments are due to a full meeting of the Standards Committee on May 20. Is that a meeting, Michelle or is it just when they're due to be input to them?

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

That's when they're due.

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

That's when they're due, okay. And then Dixie will be presenting them at a subsequent meeting. Okay, next slide please. Okay, so let's go through the review of the comments on the NPRM that were developed by this workgroup at the April 8 meeting. Next slide, please. Next slide, please. Okay, again this is a summary of the areas that we covered. We actually had two workgroup members who graciously agreed to spend some time looking at a review of our comments and our initial input against what is exactly specified in the NPRM and come up with their results and report them to us today for further discussion.

John Hummel will present first; he is looking at a mapping of our original recommendations for certifying privacy and security of HIT modules against what came out in the NPRM, so again mapping our original recommendations to what came out in the NPRM. And then we'll get some insights on end-user device encryption from Aaron Miri. And finally we'll bring up two new areas, automatic access time-out and integrity. Next slide.

Okay, so in terms of the areas that are covered in the NPRM for certification of individual HIT modules against security criteria, these are the criteria areas; authentication, access control and authorization, auditable events and tamper-resistance, audit reports, amendments, automatic access time-out, emergency access, end-user device encryption and integrity. Next slide.

Okay, so here we have a table that I believe was examined by John Hummel and John's comments in the yellow and I'll turn it over to him, are to help us understand how well the table in the NPRM mapped to our original comments. So John, if it's okay, I'd like to turn it over to you for the initial discussion.

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

Sure, what I did to go through the table, after some discussion with Dixie, was to go through and ask the question which is, take a look at like the clinical module and asking the question that approaches from the applicability of the table. So if you take a look, it pretty much matches what's in the security regs. There were just a few that were not there, for instance, in the very first box we'd take a look at clinical; they don't include integrity, which is interesting. But for the most part, it matches pretty well down the line for all the different requests that are there. So, it basically was just going through and saying, does this really...does it really work and is it applicable? And then also for the approach two, were there some places where there were just amendments and things like that. So that was pretty much it.

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

Did we lose Lisa?

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

I don't know, but...

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

Oh, I'm sorry; I was talking away on mute. I apologize. Okay John, so what I heard you say for the first yellow box it excludes number 8, integrity, is this an oversight? So it is your thought that perhaps integrity was not included purely by mistake and that there was no other explanation as to why it might not have been included, is that right? Did I hear you correctly?

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

Yes, that's correct; I think it's too important to have been overlooked, so I would like to have this re-examined to make sure that it was not done on purpose.

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

Okay, so I'd like to discuss this one with the group, but perhaps our comment could say, we believe number 8, integrity, should still be in this document and would request that it be considered for inclusion, you know, going forward; something along those lines, letting them know that it's missing, we assumed it was an oversight and our comment would be, we would advise to add it back in. So, any discussion on that? Everyone agreed to that comment and Michelle, does that make sense as far as a comment for us to make back to the...to ONC?

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

This is Steven Lane, I agree.

M

(Indiscernible)

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Aaron; I agree.

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

Okay.

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

This is Scott; I agree.

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

Yeah, this is Brian; I agree.

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

This is Peter, I agree.

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

Hi, Peter.

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

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

Okay, thank...I'm glad you could join us. Let's see, so let's move on to the next one and John's note here is excludes amendment only, is that okay? So here, did we find another perhaps overlooked or missing requirement on amendments and we would advise that that be added back in; is that correct John, is that your recommendation?

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

Yes it is because again for care coordination, excluding amendments really doesn't make a lot of sense.

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

Okay. Is everyone agreeable to that comment? It is similar to the previous comment we would state that we assume this was an oversight and ask them to add it back in. If no objections, I'll move on to the next...so here we have, in the Direct area and John's comment is that it excludes all of G, design and performance. This section also includes application access to common clinical data sets but is not context specific and it includes only security criteria. Is this okay? So John, is there anything that you want to elaborate on that or any background that can help us?

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

Well no, this was just as I read through the Federal Registry and went through the kind of each step that they try to do, it seems like they excluded it as part of the design, but I really couldn't tell if it was done on purpose that way or if it was the...were the comments put in there by design; so I was just...my questioning my own understanding of what that particular part does, the G part and then what's the specific what they're trying to do for D through 1 and 3?

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

Okay, so you're saying the requirement G, design and performance is missing. Between the lines of rows F and H there was previously a G, design and performance.

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

Right. And it's in the Federal Registry as well.

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

So it's just missing from the table?

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

That's what it looks like.

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

Okay, well that's interesting. Again then you would be assuming that this is an oversight on their part...

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

Yeah.

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

...having it in the text of the document but not in the table.

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

That's correct.

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

Okay. So our comment, I suppose, would be that we would...we assume it's an oversight and request that they add it back in or, if they would give us an explanation otherwise.

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

Right.

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

Any...is that okay as a comment back to ONC or does anyone have any other thoughts? Again John's saying that G was in the text of the document, but not in the table.

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

Again this is Steven Lane and I agree.

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

And John, this is Lisa, I just had a thought is there...was there any commentary that they thought there might be either trouble te...trouble verifying this or any thought that it wasn't strictly security related or there's no comment at all?

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

No, I think what...when I read through the Federal Registry itself, read through the entire G part, it seemed like they were trying to get to a level of specificity in terms of what the system performance would be, what this...you know, they were designing in patient safety features and things like that. So it seemed like it was not intended just to be for security, but it had some other things that would be testable criteria for certification. So to me it just looked like they missed it on this table.

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

Okay. Okay, so we will...I guess the recommendation will be to have a comment that we assume this is an oversight, we would request that they add back in the security component for item G into the table or otherwise explain why it's not in the table.

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

Yup.

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

Any objections? And thank you, Steven, for that affirmation. Does anyone object to that comment? Okay. So, and John, does that wrap up your section?

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

Yes it does. I'll just say that the leading cause of blindness in healthcare professionals is reading the Federal Registry several times is definitely it.

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

That's why so many physicians can still read, because very few of them actually read the health...the federal regulations, even the ones we're supposed to.

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

Oh my goodness, that's funny. Thank you so much John for volunteering to do that work in between meetings, we truly appreciate it and thanks for making it so easy for us to get through it. Okay, let's go to the next slide, please. Okay, and Aaron, do you cover passwords or is it just end-user device encryption that you were covering today?

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

I was actually going to cover both dimensions there, passwords and encryption keys.

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

Okay, so I'll turn it over to you, if you don't mind. Thank you.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

No problem. So just as a recap from last meeting, some of the questions and comments that were coming out from the workgroup were specifically around sort of some of the maybe lax may be too strong a word, but more of the lax standards that are out there in the market around what the EHR vendors are providing up. So it was maybe to add some more meat on a bone, per se, around passwords and encryption keys. So my takeaway was to go back and look at and try to find some middle ground there that starts to ratchet up the level of rigor around both of those dimensions. And so after discussion with Jeremy and others at the ONC and of course Lisa and Dixie, we kind of came to a middle ground here to run by the workgroup.

So on the first dimension with passwords, a lot of discussion was back towards, you know, the variability in the market of folks implementing two-factor authentication, whether it's some biometric manner, whether it's badge access, whether it's a PIN code, or what be it. And while there are a number of ways we could go about it to strengthen it, to allow to one, instantiate that both admin passwords and a system level account passwords would have to one, be enabled and then two, allow the market to sort of dictate what the password strength would be, based upon your risk assessment for the organization.

So, two-factor authentication, password length, all of that would kind of be based up to whatever your risk assessment came back with from your organization. But as long as you did something, you had something in there that was more rigorous than just having no password that would be palatable for a first iteration. Before I go to the second dimension, let me ask any questions on the first dimension?

Okay, if not, encryption...

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

...I have a question...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yes ma'am.

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

I'm sorry Aaron, this is Lisa. Had there been any thought about advising that some guidance be put out as far as the risk assessment and determination of the need for the password length or two-factor, whatever? Or is it just at this point we're just recommending what should be certified in terms of the product, what should be available features in terms of the product itself?

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yes. So naturally, being a techie at heart, I went right to the meat of trying to lay in some high rigor, but the degree of it, when you look at the market and the variability of the market say in rural America versus what maybe you have in a metropolitan area and the resources and funds available, just in general, to allow for just having the standard, just having the ability to, seemed to be an appropriate first step versus specifying exactly, you know, needs to be 16 characters long, changed every 90 days, so much entropy, whatever else. So it was really more of just the availability.

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

So it would be available and configurable by the end-user.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

By the end-user based upon whatever their organizational risk assessment came back to say they needed to do.

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

Okay.

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

Are we going to make recommendations for some of this stuff though, I mean, rather than just state flexibility, because when you say flexibility, organizations that really know nothing do things that seem very good and mean that you end up having to write things down or make things more difficult; I think that recommendations might be reasonable to come from us.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

I...

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

So Peter, oh, go ahead, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

No, go ahead please, please.

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

Well, I mean I was just...that's why I was sort of separating it into two buckets, I mean, we are commenting here formally on the certification for the health IT modules and what we think the features should be; so here saying that they have features that it could include optionally two-factor authentication, varying password length and strength to be certified in the product. But then perhaps a recommendation that ONC or someone else put out guidance for providers who are going to link their policy choices to their risk assessments. And I don't think there would be any problem with putting that recommendation in as well, I guess is what I'm saying, supporting what you're saying, Peter. Thoughts on that?

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

Thank...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Well, so what's interesting is that Peter that my first pass at it, I went along the lines of trying to say that all administrative passwords need to be 8 characters in length with complexity of upper case and lower case and special character; but again it came back to that might be too prescriptive for the market right now and it was a good discussion that I kind of had with Jeremy and team about that, that if we're too prescriptive up front, that might stifle innovation, stifle the ability for the varying providers and the users of the technology to really innovate and drive this forward. And so it was really just allowing for the ability to do so, and then take into account all the other things on the market, again like two-factor auth and others.

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

I'm not talking about rules, I'm talking about guidance; just to put in things of the nature like if you require letters, numbers, capitals, smalls and a special character, it's likely the person is not going to be able to remember their password and will need to write it down, which makes it less secure. A longer password that's easier to remember may be something desirable in most cases, things of that nature.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Oh, oh, I got you, just sort of rules of the road, yeah.

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

Well, sort of guidance for providers to make the leap from the risk assessment to the determination of their own policy and implementation.

M

That's critical that we should leave it up to the users; you give them the capability, but leave it up to the users to make the determination of what suits their workflow and their environment.

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

But it's not left up to the users; invariably it's left up to the managers of the IT system that the users are logging into.

M

Well, that's...

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

I can't tell you the number of systems I log into that...

M

That's what I meant by users, I mean the...

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

Oh, okay.

M

...systems, the organization that's implementing the system, let them make a local decision as opposed to letting us set this...

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

Yes.

M

...as a national policy.

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

Right, but there is data now, so I think that it would be reasonable to let them know some of that stuff, that's all I'm saying; some guidance because people who don't know always go for the most complicated.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

And that's fair, and I know that the ONC has some pretty good stuff out there, even the most recently updated privacy and security manual that's a...solution team they just put out there the other day. I mean there are...of information that we could reference folks out to, to get guidance on what best practice is.

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

Or we could recommend that ONC facilitate the availability of guidance and just leave it at that.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

There you go.

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

Yeah, because they can...whether or not it's going to be strong passwords as defined by NIST or something along those lines.

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

Yeah, I mean I think it...as Aaron said, Aaron's recommending that we consider saying the products have certain capabilities but the individual provider implementer should decide, based on their risk assessment, what to implement; so some guidance at that nexus might be helpful.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Right. Exactly.

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

So can everyone get behind that as far as a recommendation; would be an addition here something along the lines of, recommend that ONC consider recommend...making available some consolidated guidance on the implications of password policy implementation...make sense?

M

Can you say that one more time?

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

So in addition to the recommendation here, the sub-bullet on what the product could...should contain as far as features, we add another recommendation that the ONC should consider making available guidance on the implications of password policy and what...Peter you...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

No, I mean like best practice, I think might be the better word, right?

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

Best practice, okay.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yeah, recommend best practice.

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

Okay, that sounds good. Peter, everyone okay?

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

Yes, yes.

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

Does anyone object to adding that as a recommendation? I mean, they don't have to follow it, but it's just a thought that we convey that we are aware that providers have some challenges in this area and that they consider putting some guidance together.

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

I think that sounds good.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

That's very fair. Okay, so Lisa, do you mind me going to the second section?

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

No, please do. Thank you.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Okay, second dimension here is the encryption keys. As you recall, on last weeks, or last meeting's discussion, there...a lot of us have varying experiences with various vendors and providers that some require changing of administrative level passwords, some don't. Some leave model passwords in the system lo...well beyond go-live; I mean, there's just such a smattering on the market, so trying to tighten that up a little bit.

So what we came back with after some discussion was, again, one organizational policies around encryption keys, as driven by your risk assessment. So one, again, instantiating RA is critical to understanding what level of risk appetite you're going to have as an organization. And then, two, very similar to the first dimension, having systems that have the capability to change keys at whatever frequency, as appropriate, again as defined by the RA.

And then three, as it ties into that, there are varying levels of keys, whether its data at rest, the application layer, obviously if you change a system level password you have to re-encrypt the drive again with the new password; if you do it every 90 days, that's perhaps re-encrypting 10 terabytes of data. So, there are different levels of keys that could be implemented. But again it's back to the system needs to have the ability to give the users the option of doing whatever as appropriate, depending again on your RA. Does that make sense?

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

Okay. Discussion, questions for Aaron?

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Wow, I surely thought there would be 100 questions on this one.

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

Well first of all Aaron, it makes sense to me, I mean I have more context on the background discussion, but it makes sense to me.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

And again for the workgroup, I mean again, I started off with the very technical saying minimum 128 key, AS encryption or similar; but again, that was too prescriptive. Again it's back to let's make sure the capabilities exist, give the option to the market and then again layer in the importance of having that RA and driving home whatever your RA comes back with.

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

Yeah, and again Steven Lane, I agree. I think it's a very consistent approach and I like it.

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

Yeah I...this is Lee Jones, I support the idea of being less paternalistic and trying to allow the market to settle on things.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Wonderful. Thank you, Lisa.

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

Thank you, Aaron; thanks to Aaron and John again for taking on these tasks in between meetings. We really appreciate your work in this area and for your presentations today. Let's go to the next slide, please. Okay, so now we're going to move forward for the discussion of a couple of new requirements.

The first area that we're going to talk about is C-CDA data provenance. Next slide, please. And at this point we have Johnathan Coleman, who is the Chairperson of the S&I Framework Data Provenance Committee, is it committee Johnathan? I don't know if I got that right.

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

That's good enough. Thank you.

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

And thank you Johnathan for being with us today; I'll turn it over to you.

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

Oh, okay. Thank you. So Julie, I...how would you like me to proceed here; I have not seen these particular slides or the ones that are up right now. I can provide some perspective on the work that is being done as the Co-Chair of the CBCC Workgroup at HL7 that is actually the project sponsor for this data provenance CDA IG and that is sponsored by CBCC and co-sponsored by the Structured Docs Workgroup and the Security Workgroup at HL7 and it's one of the activities that's happening within the Data Provenance Initiative of the S&I Framework. But, I don't know, Julie, were you going to go through these slides or do you want me to hack through it?

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

I think for the slide that's up right now, it's just going over like a history of how we got here. Are you comfortable with that?

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

Yes, certainly.

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

In terms of the...and all that, yeah.

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

Yup. All right, well not knowing what slides are ahead of me, I'll do my best. So Lisa, tell me to speed up, slow down or be quiet as needed. So a little bit of a historical context here; I think most of us remember the PCAST report and within the PCAST report there were certain recommendations for addressing metadata, security metadata, privacy metadata included and they were addressed in part in the data segmentation for privacy work, but provenance was also listed and provenance was not really picked up, at least in the Data Segmentation for Privacy Initiative at that time. So this current effort is building on that. The Standards & Interoperability Framework has an initiative that is dealing specifically with multisource CDAs and exchange of provenance information between EHR systems and then ultimately between EHR systems and other devices such as patient-generated data in PHRs and so on.

As part of that effort, ONC proposed a project through HL7's Community Based Collaborative Care Workgroup to develop a specification or a standard that will pull in and clarify some of the existing provenance requirements that are there in the CDA and in other specifications that exist within HL7. So, the project for the HL7 Implementation Guide for CDA R2 was released, it looks like...I'm not sure about the underlined and there; the full name for the specification that was proposed is the HL7 IG for CDA R2 Data Provenance Release 1. So that is all one document or one specification and I think that's the one that the NPRM is seeking comment on.

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

That's right.

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

Okay. So if there are no questions on that, we can reveal the next slide, please. Okay, now these ones...I'm good with these slides. So, I think the...these bullet points talk to the maturity and then there is some follow up material. So this is a new standard, it's a new specification, but the scope of the project that develops...that is working on this standard was to combine and compile existing provenance information from related specifications.

And there was a landscape assessment done and the community members within the S&I initiative provided a number of standards that were potentially important or related to data provenance. And I think that we identified 11 of those standards just within HL7. So this project, while it's a new standard, it was designed to capture provenance requirements, provenance conformance statements from the base CDA, from the Data Segmentation for Privacy, normative standards in HL7 and other standards that are already in existence and have provenance related capabilities.

So the design for this implementation guide, so the standard is an IG, is that it contains templates that describe how to use the provenance capabilities from those existing standards so that they can be overlaid to the CDA and used as a baseline for making sure that provenance information is appropriately

captured, constrained and communicated; so in terms of maturity, it's a new project, it's a new implementation guide, but it is a combination and a compilation of existing provenance material from a number of different standards within HL7.

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

Johnathan, this is Lisa. I just had a quick question as to whether this initiative is taking into consideration the recommendations of the Task Force that we had under the Standards Committee in January, as to the scope of the use case, but also the type and nature of provenance data to be carried, including the fact that we recommended that it include source information as well as whether and where and when the data was changed, you know, that kind of recommendation that we provided in January.

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

Um hmm.

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

Was that...is that part of what is being considered by this initiative?

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

It is, it's very much so. So, the recommendations that the Task Force provided on the Data Provenance Initiative within S&I were taken on board by that initiative and absolutely factored into the work plan and that extremely informative and useful guidance has been used to shape the way the initiative has been moving forward since then. This...just I think maybe a point of distinction here, so the HL7 IG for CDA on Data Provenance is one of the candidate standards or potential standards that that initiative may use. But the NPRM is looking for comment on the CDA IG for data provenance that's at HL7, I think rather than the ongoing work of the S&I initiative; does that make sense?

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

It does make sense, I just have a question of do you know why they are asking for this...comments on this specifically? Is it because they already got comments on other things or is there another reason?

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

I...my personal opinion here is that this is the Meaningful Use standard, the CDA and the Consolidated CDA is the baseline that's already in certification criteria and we have no single point of reference on how provenance information should be captured and conveyed with CDA or Consolidated CDA. And so this specification is designed to give that clarity and put together a more discrete and cohesive set of templates for that kind of interaction.

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

And that's something that could be certified in the health IT module.

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

Correct.

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

Okay, that's where I see the distinction. Okay, thank you.

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

Than...absolutely. So, I guess the short answer for me on maturity is, yes it's a new standard but it's based on existing standards, many existing standards and rather than having to search around and find the provenance related information from all of those different standards, this standard pulls them all together and puts them in one place. So there shouldn't be a whole lot of new material in this particular standard, even though it's a new standard in itself; it's a standard for implementation guidance. So, next slide, please.

So why are we doing this, and I think Lisa, this maybe gets back to your earlier question. As you noted, the Data Provenance Initiative highlighted a number of different functions that have provenance related events and this particular specification in HL7, while it's dealing specifically with CDA, is addressing some of the functions that different participants in the lifecycle may have. And there are a couple of examples here on the slide and there are more in the specification. So, one of those examples is assembling.

So if there's clinical information that exists on a particular patient or to do with a particular encounter, there may be an algorithm that takes that information and assembles a new artifact, a new CDA based on some predetermined formula like, let's take everything that we've got on this patient and put it together in a new document, right? So that would be a predetermined query for creating or assembling this new artifact. Whereas a separate function and a distinct function could be composing where there may be some more active human participation and that somebody might choose or cherry-pick certain pieces of information to put into a new CDA. So let's say, we'll choose that piece of information and that one, and so that's a judgment call and that particular act of composing derivative information from multiple sources might be reflected differently from a provenance standpoint.

And so this specification aims to help identify those types of different participations that may be involved in creating artifacts so that the end consumer of that information, of that CDA, for example, would know whether or not it was created by a machine from all the information that was there, whether it was created by a person and ultimately where the information that's in this new artifact originally came from. Did the heart rate information come from a Fitbit or did it come from an FDA approved medical device? So that's really, I think, getting to why this project is in place and what the real world problem is that this particular project is trying to solve.

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

Okay, let's pause there and see if anyone has any questions about this that perhaps Johnathan or I or Julie could answer.

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

I didn't understand it enough to even ask questions for a lot of this. Am I alone in that that this is like over my head?

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

I'll join you on that; this is Steven Lane. I think as a clinician, I must say I don't fully understand the subtleties of this. I mean, it makes sense at a high level.

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

So this is Johnathan, that's...I get that. So I think the next slide is the one that talks about the usefulness and maybe that will shed some light and perhaps we should have led with that slide. So I think if we could advance one slide, Lisa, if that's okay with you.

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

That's perfect. Thank you. Next slide.

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

Yeah. Okay, thanks. So the purpose behind this is, if we have the ability to know where information originally came from, the clinician or the provider may be able to turn around and say, I'm going to trust that heart rate information that came in from the pacemaker over and above the information that came in from the Fitbit or the new Nike running shoes or whatever they happen to be that measures the same thing, but not necessarily to the same degree of accuracy or reliability. And so understanding and being able to retain the provenance and the original source of that information all the way through as it is reused and put into new documents becomes important. And so this specification is intended to help with that particular issue.

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

(Indiscernible)

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

We have...I'm sorry, go ahead.

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

I was just going to say, that makes perfect sense, even to a clinician.

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

Okay, great.

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

I agree; this is Peter.

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

Yeah, I was going to say that part of it the clinician is the sort of end-user of this; I mean, it's...well it's clear that the providers would prefer to know the original source of the data as opposed to just it's all in a C-CDA and you don't know where it came from, it's just all in there. If you...as he said, if you were to know that heart rate data came from a pacemaker as opposed to a Fitbit, you would...that's information that's valuable to you at the point of care. And there are a bunch of standards out there that provide ways to do this and the HL Data Provenance Implementation Guide Initiative is to allow us to implement that in the health IT module in a way that sort of gathers all information from existing standards, but also perhaps has some templates for some use cases that would be useful. Did I get that right, Johnathan?

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

You nailed it, thank you, Lisa.

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

Can we go to the next slide, please? And so this is where...this is a concise statement of what ONC is asking us or asking the public. We need to weigh in, if we can, on the maturity and appropriateness of this initiative and then also the usefulness of an implementation guide initiative like that to the certification initiative for health IT modules such as...what's ToC?

W

Trans...

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

Its transitions of care and then...

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

Transitions of care.

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

...the VDT is the view, download, transmit.

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

So, transitions of care via C-CDA or maybe some other document or the view, download and transmit, which I believe is primarily focused on the patient having access to their data. The data that they could access would have provenance information associated with it in compliance with this implementation guide project.

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

Right.

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

So I think I can speak again with the clinician's perspective; I don't think there's any question that those of us who receive these through transitions of care and speaking of patients who receive it as VDT. I think having provenance information that is readily accessible and presented reliable, standard, etcetera is a good thing. So I think having an implementation guide would be very helpful when the standards are sufficiently mature. So I guess I'm a little stuck on question one, how do we as a workgroup educate ourselves, maybe the rest of you are already educated about the maturity of these standards. But certainly once they're mature, I think that they should be included in transitions of care and VDT criteria.

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

So this is a question...this is John Hummel, a question for Johnathan. I'm assuming that we're using the HL7 2.5.3 that's currently used for Meaningful Use criteria? So...or are we looking at a future HL7 like 3.0?

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

So this is, it's probably better for HL7 to answer that directly, and I can get you an authoritative answer; but my understanding was that this is based on the CDA R2 and that the provenance information that exists already in CDA R2, DS4P and other normative HL7 specs, and by...I'm using the term normative as final, balloted, approved and hopefully in use. And that this is an overlay that gathers all of that stuff and puts it in one place. So it's applicable to V2...to CD...excuse me, to CDA R2.

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

And so I think...it's been my experience working on a lot of these other bases that that's a fairly mature process when they get to the point where it's published in the R2...

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

Correct.

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

(Indiscernible)

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

Yeah, they're not draft standards, they're final standards...

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

Yes.

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

...that are normative and approved. Yeah.

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

Now we do have the methodology that was developed by Dixie and others that the Standards Committee adopted for measuring or quantifying the maturity of a particular standard and perhaps an

exercise between now and the next meeting is to take...to apply that process or that evaluation to the standards that are being included in this HL7 implementation guide effort, to actually gauge the maturity of them based on the process that we decided on earlier at the Standards Committee and then report back. Michelle, Julie, does that make sense?

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

I think that's a good, logical way to do this and I think it would provide the workgroup a little more time and visibility into the IG itself to be able to make that determination. So...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yeah, this is Aaron, I agree with that. I mean, I...as a CIO I look at this and I think, transparency is always key and I think the more the merrier, especially for our clinicians. But I also wonder about the maturity of the market and the products on the market today have the ability to transmit that so we could capture it. I mean, I don't know, so...

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

Yeah. So this is Johnathan, just if I may comment on that. So, and I'm sorry if I fumbled it a little bit earlier. So this specification is the template which describes how provenance is captured for the CDA, which the CDA is the foundation of the C-CDA, right, which is already included in Meaningful Use. So there shouldn't be anything new or earthshattering in this implementation guide that they're seeking comments on because it's based on and inherits all the backwards compatibility to the base standard that's already in the certification criteria.

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

Okay, so...this is Lisa. I think that we have a general notion today that this...these standards sound like a good idea, but perhaps we need to do a little bit more analysis with regards to the maturity of the inputting standards into this initiative, we could take a look at Dixie's model for determining maturity. And then with regards to the usefulness, the second bullet, in connection with the certification program, just to check to make sure that we understand how this traces back to actual certification requirements and whether we're agreeable with that. Does that make sense to everyone?

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

Yes it does.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yup.

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

So, we're going to have to do some work in between now and the next meeting. This is certainly something that I can work on and Dixie as well, I'm volunteering her, but knowing that she's the person who's most familiar with her process for determining maturity or expressing maturity, I would certainly enlist her help. Is there anyone else interested in working on this between meetings so we can come up with a recommendation to the workgroup for approval for...at our next meeting?

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

Lisa, this is John Hummel and I'd like to be part of that because I think I have a better understanding of HL7, based upon the work that we've been doing, building all sorts of interfaces up here.

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

Okay, thank you, John. Anyone else?

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

Lisa, this is Johnathan, I'm not on the workgroup, but please feel free to reach out to me and use me as a resource anytime you need to in support of this effort.

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

Okay, thank you very much everyone. And Julie, is this...does this make sense as a next step for us to work on in between meetings as far as you're concerned?

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

Yes, because it actually...it's good to come back to it during your May 6 I think is your next meeting.

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

Right.

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

You can take this up in the beginning and then it ties in quite nicely, I would say, to DS4P. So...

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

Which will be on the agenda for the May 6 meeting as well; that'll be like a new topic, right?

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

That's right, that's right.

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

Okay. Okay, so what Julie's saying is this ties in to the Data Segmentation For Privacy topic, which we'll be taking on on May 6. So it'll allow us some time to get a little more depth on the recommendation and a little more understanding of the background and also segue nicely into a new topic. So unless anyone has any further questions or objections, we will move forward with developing some more in

depth...well doing some more in depth background work and developing a recommendation for the workgroup's consideration at the May 6 meeting. Okay. Next slide, please. Next slide, please.

So I'm assuming we're okay on time, we're going to keep plodding forward. Our next area of criteria for consideration is auditable events and tamper-resistance. So the NPRM proposes no change to what was in previous versions as far as the auditable events and tamper-resistance criterion; but is asking us for comments or input on some specific questions. Okay, so, let's see, let me look ahead at the next slide for a second. Okay, so I think Julie we can go on to the next slide, right, and start considering the questions there.

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, that's right.

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

Next slide, please. Okay, so changes in user privileges. ONC seeks comment on whether they must explicitly modify or add to the overall auditing standard to require change of privileges to be an auditable event or if this event is already audited at the point of authentication. And are there any standards out there that we know of that we could recommend to be used in order to facilitate the recording of these additional data elements?

Okay, so I think the question is when we consider changing of privileges, do we recommend that that's an auditable event? Is it already audited at the point of authentication specifically? And do we know of any standards that are applicable here? Any input on this?

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

The privileges that we're talking about these are privileges of the individual user...

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

Yes.

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

...to utilize or access data in the system?

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

Correct. So at the point of authentication, that's what we're talking about. And here, whether there's a change by let's say the system administrator ad hoc to a specific privilege, is this an auditable event or is it typically audited at the point of authentication? And what would we recommend?

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

You know, it's an interesting question because, I mean, I've never really thought about this. I mean, when I log in onto my system on Monday, I have a certain set of privileges and security access, if somebody makes a change in the back end and on Tuesday I have access to something different, more, less, I don't know that that's recorded at the time of my login but somewhere in the system audit trail

one can probably determine that my security on Monday was A and my security on Tuesday was B, but it's...I don't know, do any systems actually sort of capture that at the moment of login and record that? I wasn't aware of that.

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

Steven, yeah what EPIC it does is it monitors your role, so role-based security. So if I was adm...your administrator for your EPIC and I went in there and changed your privileges from CPOE to only view documentation, there's an audit for that. So I can go through and take an extensive audit for any of my users that are on that system and see if anybody's changed their privileges and that's just to make sure that we don't have somebody going rogue out there and start ordering meds.

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

Yeah, no, no, I understand that John, but here it says at the point of authentication. So when I authenticate on Tuesday, does the system say, Dr. Lane authenticated in this particular role; because it seems to me that those are separated in the audit trail.

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

This is Scott and it's not clear to me whether what's being asked here is whose authentication; is it the authentication of the user whose privileges have changed or is it the authentication of the admin who made the changes?

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

I think it's the...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

The user.

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

...user, but, it's asking us do we know when it's typically audited, why...when it's changed by the administrator and/or at the point of next authentication.

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

Well I read this a little differently. I look at the point of authentication is that when I grant access to a system, I have to first authenticate that person to give them the access and then based upon their role is what access I give them and so to me those...when the user logs in, they're authenticating to the system, but I've already authenticated them, based upon identity before giving them access.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

This is Aaron, let me ask you a question. Let me just take this point a little bit different. So I'm a user, I log in to a system and as...and usually, usually the system administrator, the person on the back end is different than the actual say clinician using the actual application, right? So administrator makes a change in my password, or change in my system level accounts rather, I log in and I expect to see things differently, based upon whatever I requested, and hopefully I'm aware of the change. At any time do you get a prompt, in any of those big EHRs, and I'm a user of all of them, saying, hey Aaron, your permissions have just changed? Is there any level or point that I am participating in that agreement of my access has changed?

Because the way I read this question is that that's what they want is they want awareness not just that your stuff has been changed, but that the user knows that I have changed. So therefore it's logged, audited and grabbed but there is implicit cooperation and you're part of the story, per se.

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

Yeah, I don't...I'm not sure about that latter part, I really...I'm really not.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

That's the way I read it is that I think this just gets back down to granular control and that you're aware of what's going on around you.

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

I mean, is it the thought of the workgroup that we should seek clarification on the question?

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

Oh yeah, I think...

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

Because I believe that we can get it. Julie, is that within the realm of possibility? Julie?

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

Oh yes, yes.

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

Okay, so we can formulate a question to send back to ONC and say, we'd like to give you input, but we need some clarification on the question. Now do you know Julie or Michelle if they can actually provide us this while the NPRM is out for comment?

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

Umm, I think so. I think if it's a clarification on what the question...the language of the question is, I believe we can give some guidance on that.

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

Okay. So we will ask for clarification on this question, including some of the notions that Aaron added and then...because I think it's a good point that most of us hadn't thought of and so we can go ahead and say, this is...these are the things that we talked around, but we'd like to know exactly what you mean. And I also think for John and others who are involved at this level, is there any standard that you know about that are applicable here?

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

There's...yeah, there's NIST 63-3...2 or 3, they just revised it like a year and a half ago.

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

Yeah, it's dash 2, I think. Yeah, so that's...well, you know, they typically consider those NIST documents to be guidance, so I think we can certainly suggest that, but are there any standards anyone knows? Johnathan, any normative standards here?

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

So this is Jason. So we build a lot of these systems, it's not so much a standard like the NIST document, but more a commonly accepted practice. There are a whole set of controls around detection of change; so it isn't necessarily this specific type of change, but for example if somebody were to elevate their privileges to a domain admin, there should be an audit that gets written there and somebody has to have a control that detects that. So it may not simply be that the end-user going in is alerted that their privilege profile has changed, but somebody in the backend becomes aware that something changed and you'd want to be able to reconcile that change with the change request, right?

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

Right.

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

So there are a lot of standards around that, when a change is requested it's got the appropriate authority, and then the change is detected and then you can reconcile the two it's fine; but when you have that change without any of the background request and approval process, that's when you know you have to have something anomalous and further investigation.

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

So when you say there are lots of standards out there, is that something you can dig up for a few recommendations for us to give to them?

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

So far again, for the systems that we build, they tend to be federal, but there's a whole control family within the 800-53 around change management and configuration of that.

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

Okay.

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

Yeah...

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

This is Johnathan; I concur with that and I know that NIST guidance documents are guidance generally, but they're required for federal information systems that have to go through certification and accreditation. So, they're an excellent source of the specific audit controls right there. And as far as the interoperability standard that comes to mind for audit, there's the IHE ATNA audit trail and node authentication standard, which I think describes...

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

Right.

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

...some of those system events which may be used, but there has been some work on that fairly recently, I think but that may be one that's worth looking at.

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

Yeah, I think I recall that being recommended before, a couple of years ago, that we tracked what ATNA, the ATNA specification from IHE. So...I'll take a look at that offline as well and talk to a few folks. I want to go to the next slide because this is...the next slide represents more questions that ONC has around the audit log.

Umm, now it seems to me we've...I mean, I know I have seen these types of questions before and that ONC has gotten some input on it, but maybe one of my homework could be to go back and look to see where we've provided recommendations like this before. But, is there a critical subset of auditable events that ONC should require be retained...remain at all times? And are...is there additional information regarding what those events are? What are the critical ones and why are they critical? And is there any other approach that ONC should consider? And are there any other...any possible negative consequences that could arise from keeping a subset of the audit log functionality enabled at all times?

Now I think we also had a question about whether or not the audit log should be allowed to be turned off altogether, so it seems like a multi-layered question. But, I'll leave it out here for discussion. Basically they're asking about a critical subset of auditable events that should always be on. And if...is there an alternate approach to that and also are there any negative consequences of doing something like that, in the specification of the certification requirement.

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

So Lisa, this is John Hummel again. In California we have a California law that went into effect January 1, 2012 which is SB-850 that requires to have any clinical changes made in the EMR has to be auditable and it has to be kept and retained; so if I make a change to smoking status, it has to go in there and tell me why I made the change, when I made the change and who made the change.

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

And is that the only element that is required to be maintained as critical?

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

Umm, yes, currently the state law basically says, anything that's clinical and there's a pretty broad range of things you have to monitor for that, but it's not required for any of the business functionality for like patient bills and stuff. But if it's in the chart, they want it kept as an auditable and it's supposed to stay in there forever.

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

So I think the key distinction there...this is Jason, again; is whether the value was changed versus simply viewed, to your question about criticality.

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

Yup.

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

It's one thing to keep track of who saw what, but it's also another...it goes to materiality and we can be compromising somebody's care if we change their blood type or whatever, right; the integrity component.

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

So and what about the VDT, the view, download and transmit, any functions that help accomplish that.

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

Well those are in your standard audits, because if anybody...yeah.

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

I think the question is, what is the standard audit set? What is the critical subset, if any? And John has proposed that there is one specific one which is a change to a data element in the clinical record. Is there anything else around access or authorization or privilege? I'm just throwing things out there, but...or are there any standards we know about or anyone that we know that takes an approach that says that some subset is a critical set that cannot be deleted and always must be maintained?

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

This is Steve...

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

Sorry. Again, so one of the other approaches that some of the consortiums that we work with take, and this is most of the states have taken this approach, they make an important distinction between the type of data; so if it's information in the claims side, it's your home address, that's less important than the clinical data. So if you're worried about performance impact on the system, if you're worried about log volumes that are exceeding your ability to retain or store or analyze, those are the kinds of compromising that they're taking, is focus on...it's not just that it's an action that's critical, it's that action on the type...a certain type of data.

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

Steve, this is John Hummel and I think that...are you guys up on using on First Doctor or eScribing for scheduled drugs?

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

And you were...John, you were referring that question to the last speaker and I think that was Jason. Was that Jason?

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

I was trying to see if Steve knows whether or not...

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

Steve, are you there?

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

...because the way that we've been using First Doctor in our key system up here is that you have to go in and put in the RSA token number and then that's recorded separately, in terms of the database as proof that that was a doctor and the doctor was identified through the RSA token.

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

Yeah, two factor authentication is required for UPCS...are you saying First Doctor or Doctor First?

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

Doctor First.

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

Oh, okay, don't make that mistake...never...bu...the DEA really micromanaged this, this is kind of what we were talking about earlier about trying to be flexible and allow people to be creative and more modern. But the DEA specified things so strictly for the controlled drug ePrescribing. If we're talking about auditing, I think that the auditing and the controlled drug ePrescribing is a model probably not to follow, although people are welcome if they want to. It's extremely strict and auditing means three different things in the DEA's regulations.

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

I was just thinking that in terms of this particular question in that it's...now it's another part of my audit that was not part of the broad audit because I implemented that type of prescribing.

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

Right. So, they do also ask whether there are any negative consequences for keeping a subset of log functionality enabled at all times? And I think that's because they've heard a lot of input when it comes to should the practice be able to turn off their audit log and I think they got enough input on that to really understand that there are times when it may need to be turned off for system maintenance or some other kind of errors or overflows or lack of storage or whatever. But then when you consider having a subset that's always required to be on, does that have any negative consequences? And would

we say it's the same negative consequence for having a whole log enabled instead of here the question is, for that subset, are there any negative consequences of keeping that enabled at all times?

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

The only thing that I can think of that would be negative would be disk space.

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

Well I mean...

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

...this audit, you've got to have a log, the logs going to grow, so...

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

I mean here...it's also about you almost are you taking away the ability for the local decisions to have the audit logs completely turned off.

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

Huh.

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

So, I just know that there's been a lot of input that that should be a policy decision, that should be something that's left to the maintainers of the system and if that's the case, then it's the same question for the smaller subset, do we really have to have it all the time? So John, in your case with the California law, it's potentially saying the log needs to be on all times and it needs to be capturing at least that one data...that one auditable event.

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

That's correct.

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

Have you seen any negative consequences related to that or any rationale that's been presented that that's a bad idea?

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

No other than a couple of vendors were caught off-guard and they didn't have auditability when that log hit and so, that's been about the only negative thing I've seen.

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

Okay, any other thoughts or input on this item? Okay, so between now and the next meeting we'll work on this, but if anyone has any thoughts about other data elements that should be part of a critical subset, talking to people or doing some background research if you come up with anything, please let us know. Okay, next slide, please.

So that brings us to the end of our discussion on the topics for today. That doesn't mean we're done, we have to develop draft recommendations between now and the next meeting and present them at the next meeting. But as far as the discussion, is everyone happy that we've done what we could do today?

Okay, so the new topics that we will introduce at next...at the next meeting include Data Segmentation for Privacy and Electronic Submission of Medical Documentation. And I would say that there is significant amount of background information on both of these topics. There's been work from the S&I Framework and others on DS4P and also we on the Standards Committee have had several presentations regarding the Electronic Submission of Medical Documentation and I believe that the Standards Committee as a whole gave that group feedback formally and so perhaps we can dig that up and provide it as background information for next week.

And then we can get to the matter of the specific questions that they're asking around security certification so having that background I think would be a nice addition. So Michelle...I mean, Julie, is that something we could take a note to dig up? I think it's in the last 6 months, but I think we've had at least 2 updates on this project and we've...and I believe the Standards Committee provided formal comment or provided comments at the meeting that were documented.

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

Yes and Lisa, would you like that as read ahead for the meeting?

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

Yes. Most definitely. Yes, most definitely. Okay, Julie, do we need to go through any of the backup slides or are we good?

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

Umm, I think we're good; that was provided for extra information for the workgroup members.

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

Okay.

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

Yeah.

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

All right, so any other questions, comments, thoughts? Everyone clear on where we are in our project and what next steps are? Anything that we can do to help facilitate moving forward, let's open it up for the group. Okay then, Julie and Michelle, 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. We have no comment at this time.

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

Okay, well thank you, Michelle, thank you Julie and thanks to the members of the workgroup for your participation today. Again, special thanks to John and Aaron for their work in between meetings and for the work we're all going to do going forward. I'm looking forward to continuing our work with this group and we do have a full Standards Committee meeting in person in DC tomorrow; I look forward to seeing some folks there and I look forward to talking to you all on May 6.

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

Thanks, Lisa.

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

Thanks, Lisa.

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

Thank you.

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

Thanks Lisa.

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

Okay, bye, bye.

Public Comment Received During the Meeting

1. (8) Integrity does not have to be in the Clinical 170.315(a) group because Integrity is related to transport / exchange of information. The Clinical group does not get into the exchange of data.
2. (4) Amendments is a criterion for patient engagement of providing information about incorrect information in their EHR. I think it may be an oversight in 170.315(e) Patient Engagement, as well as, in the 170.315(a) Clinical.
3. The current C-C-DA is R1.1. This proposed IG is for C-CDA R2. There are issues of backwards compatibility of R2 to R1.1. So, this IG may cause a burden to the industry having to deal with documents in C-CDA R1.1 & C-CDA R2.

4. Yes: If a user's profile was changed, this should be auditable. Different profiles allow differing views and differing ability to carry out certain tasks. When the user authenticates (logs in) the user is not typically told (nor can see), that their level (profile) of access has changed.
5. Slide 18: The Audit Log should not be able to be turned off.