



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
March 25, 2015**

Presentation

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

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

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

I'm here.

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

Hi, Dixie. Aaron Miri? Boban Jose? Brian Freedman?

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

Here.

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

Hi, Brian. Jason Taule?

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

Here.

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

Hi, Jason. 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? Peter Kaufman?

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

Here.

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

Hi, Peter. Scott Rea?

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

I'm here.

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

Hi, Scott. Sharon Terry? And Steven Lane? We can get Steven back. Okay, and from ONC do we have Jeremy Maxwell?

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

Hey Michelle, I'm here.

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

Hi, Jeremy. So again, thank you all for your patience and I'll turn it back to Dixie.

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

Okay, thank you Michelle and thank you all for yes, yes, that was patience beyond the call of duty. So we really, really do appreciate you taking the time to dial in. We'll try to be as efficient as possible with your time today. There is...the only topic on our agenda today, you can go to the next slide please; is review of the...review of our draft responses to the questions that were asked of us regarding sections E and F, and then we're opening...well, then initially actually we will be discussing section G, which has to do with consent and so we'll be crafting our response to the three questions that were asked about section G. There...our comments and recommendations will be presented at the April...to the Standards Committee meeting...to the Standards Committee at the April 22 meeting. Next slide, please.

Okay, next slide. Section G...section G asks...all relating to consent. What standards should we put forward in the 2016 Standards Advisory for basic choice? Secondly, how much work should ONC be doing on other standards while clarifying permitted uses? And the third question is, if standards development needs to be done, what should we be working on? And they used as an example data segmentation for clinical decision support, similar to data segmentation for privacy. Next slide, please.

Before we get into this discussion, I wanted to, for those of you, just to remind you what the roadmap talks about in...with respect to consent, the roadmap talks about two types of consent; one called basic choice and the other called granular choice. And basic choice they define as the choice an individual makes about the use and disclosure of the health information...of their health information generally, including electronic exchange of health information that is not subject to heightened use and disclosure

restrictions under the state or federal law. And I want to remind you that in accordance with HIPAA, an individual does...a provider does not need an individual's consent to share health information for the purposes of treatment, payment and healthcare operations. So if there needs to be sharing of health information for the purpose of treatment, for example, there's no consent needed nor can the individual restrict access to their information when it comes to treatment.

The second type is granular choice. And granular choice does not relate to treatment uses, granular choice...or general treatment uses. Granular choice refers to the choice an individual makes to share specific types of information including information that fits into categories to which by law, protections in addition to HIPAA apply. And secondly, the choice afforded an individual based on their age and third, the choice to share health information by specific prider...provider or payer types. And this is consistent with the individual choice principle of the Fair Information Practices Principle; so granular choice really applies to things like the Part 2 data that restrict access to information that has to do with substance abuse or behavioral health.

So granular choice is really applied more to where the law requires that an individual be given granular choice. And in general, you know, general for treatment that doesn't apply, but in specific cases where the law, either state or federal, actually articulates specific granular consent, then that's where the granular choice is applied.

So, the first question they ask us is what standards should we put forth in the 2016 Standards Advisory for basic choice? That's basic yes/no basic, you know basic choice for the ability to use one's health information. So basic choice, the choice an individual makes about the use and disclosure of the health information generally, which is not subject to heightened use or disclosure restrictions under federal or state law. Okay, do we have...now the only, actually the only standard...there are two standards that I know of that address choice, and both of them are actually in development, they aren't mature.

One is the UMA profile of OAuth 2 where UMA stands for User Managed Access; and UMA allows an individual to make their personal preferences known through the OAuth 2 mechanism. But as I say, UMA is in development and it's a profile of OAuth 2. The other is I know that Health...HL7 has some attributes that they've defined that relate to consent, but I believe that that work is still in development as well. Do others of you know of standards that directly address consent or basic choice? The DS4P, which is an HL7 standard now, relates to data segmentation, but not to basic consent.

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

Dixie, this is Scott and there is some work to do standardizing how consent is captured and perhaps managed over time, there is some work that's going on in that space in OASIS, I believe. But I don't know that that's really the question that you're asking. I think you're asking if there are standards specific to basic consent, right.

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

No, no, not just capturing, but also yeah, how they have...like the HL7 standard that I mentioned is exactly that, it's about how you capture...electronically capture consent; so that would be applicable.

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

Yeah, so I apologize for not knowing in advance, but I can send details to you later; OASIS does have a working group that's looking at this right now.

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

Okay, okay. Now I think that UMA is somehow tied to OASIS, too, but...

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

Yeah, I believe you're correct.

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

Yeah, that might be what you're referring to. Now is XACML an OASIS, let me see, who made...who XACML, who developed XACML? That's not really consent though, that's access control. But yes, if you can send us...I suspect that's UMA, but if you can send us information on that, that would be useful. I also know...I'm involved in the Global Alliance for Genomics and Health and they have a task force, which relates to both clinical data and genomic data. But they have a task force that's looking at looking for standards for computable consent is the term that they use, but basically exactly what we're talking about here, how to electronically capture consent.

So I don't think that there are...I think our answer should be that we know of no mature standards that are able to electronically capture or represent consent. But we know of efforts, and we should mention OASIS and HL7 as efforts that are working on it. Does that make sense with everybody?

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

Yup.

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

Okay. And Jeremy, did you guys get that?

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

Yes, yup.

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

Okay. Let's go to the next part of this one then. The second question is how much work should ONC be doing on other standards while clarifying permitted uses? I guess this would be how much work should ONC be doing on any standards while clarifying permitted uses? And if standards development needs to be done, what should we be working on? Does anyone have anything to say there?

If...of these efforts that we're identifying, certainly ONC should be encouraging and engaged, I guess...should be encouraging and engaged in existing efforts? Because this is, you know, maybe what we should say is that we recognize the importance of being able to capture consent electronically. I've been in conversations before, I recall in the Privacy & Security Tiger Team, for example, where people were talking about exchanging consent electronically, but what they were talking about is stuffing a PDF of a signed consent into a CDA, for example, and I think that we should articulate the need for real...really capturing consent electronically and not just a PDF. Do you guys agree?

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

This is John Hummel and I'd agree with that.

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

Okay.

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

Yeah, this is Brian. Would we also want to mention something in regards to like instead of it being a PDF, maybe being more specific like talking about like in discrete data fields or anything like that?

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

Yeah, defining discrete...yeah, describing discrete data fields, just, yeah, defining the attributes, which is more what HL7 is doing.

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

Um hmm.

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

Yes. Yes, definitely, computable...

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

Okay, great.

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

...discrete data fields, yes. And especially data fields that are needed for mediating access, you know, those data fields that you have to consider to determine whether sharing is allowed or not. Not just informative data fields, but data fields that are really essential to the...to access mediation.

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

Right, yeah, I agree.

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

Okay, are there other...now the DS4P, which is Data Segmentation for Privacy, that was a...that is a profile that was originally developed by the Standards and Interoperability Framework people and then handed over to HL7 to be made a standard and maintained it as a standard. And it is specifically designed for Part 2 data, to segment out the Part 2 data which is substance abuse, behavioral health has restrictions, the law restricts further sharing, secondary sharing. Is that actually in use anywhere, do we know that? I know it was given to HL7, probably...

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

So Dixie, this is Jason Taule, there was another related effort with SAMHSA called Consent2Share and it's essentially an outgrowth of the DS4P program and that is in pilot.

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

It is...it does use DS4P?

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

Yes ma'am.

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

Ah.

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

So if you look at Consent to Share with the number, C-O-N-S-E-N-T, the number 2, Share, you'll find a bunch of links on it. So again, it's under OBHITA.

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

Under what?

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

OBH...it's called OBHITA, that was the contract, but its Substance Abuse and Mental Health Services Administration, because obviously they have a lot of 42 CFR data.

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

Okay, so maybe what we should say is that ONC should follow that and capture lessons learned from it or something. Is ONC involved in that Jeremy, do you know?

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

Yeah we are currently tracking it.

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

The reason I think we should definitely point to it is that it acts as a shim between an organization's existing EHRs so that organizations who otherwise might not take advantage of the benefits of the electronic exchange, can do so by parsing the data. So, whatever form it looks like, it doesn't require that we have to necessarily change the existing EHRs that we have.

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

Hmm, okay. And I should have checked this before this meeting, but the new...I did notice that the new NPRM has a section about data segmentation for privacy, but I haven't read that section. Jeremy, do you guys know what that says?

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

Ah yeah, so the NPRM has a section in there about being able to send and receive documents that have the data segmentation for privacy metadata as defined in the HL7 standard.

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

So in other words, an EHR module...a vendor can submit an EHR module and have that capability certified?

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

Correct, yes.

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

I mean that's another data point that ONC might want to follow is how many vendors actually submit EHRs? I mean they certainly can gauge the usability of that standard based on...get feedback from those vendors, it would seem anyway. So the...what should we say about the SAMHSA pilot?

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

Good question, I would point to it and maybe even ask for a briefing from some of their leads, Maureen Boyle was one of the key leads. And the last I knew that they had created a separate project called Project LIFT and I think that was to try to take it into greater pilots, more than the one that had originally taken place early last year.

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

Okay. So maybe what we do is we suggest that...recommend that ONC track both that and the certification...the products, you know, the certification of the DS4P capability and derive lessons learned from both. Okay. I also know that there are technologies, and I should say before I begin, one of my clients is a...has software that does probably the most advanced capability in electronic consent, used fairly extensively on the research side of things. So technology does exist in this area, so I think that maybe just following the development of technology in this area might be something we might want to recommend as well.

As more of these products come out...like oh, give you a good example, ResearchKit that Apple just announced, that has embedded electronic consent, as you may know, Sage Biometrics developed the Apple App that does...that captures consent electronically for those mobile Apps. So I think those...we are likely to see more and more products and open source code and...that becomes available for electronic consent.

And I think it's important that ONC follow that as well, because it is starting to come out more and more, very...the Apple ResearchKit and the Sage Biometrics App captures consent for sharing of the data that a particular App actually collects. So if you've got a Fitbit App, let's say, then the Sage Biometrics icon comes up and says, do you want to make the data available for research, yes/no; but still, that's electronic consent and certainly is a step in the right direction that can be used to inform further work in that area, I think. Okay, does anybody have anything else to say in this area?

Okay. Let's go...let's just proceed then, go to the next slide and review the...our draft recommendations for both sections E and F. Let's go to section E...well, section E first, actually. Can you advance a little bit? Maybe we can go past that pretty quickly. Section E, we've presented these draft responses to the Standards Committee last week, so we should be able to get through this fairly quickly; but to remind people of what we said. Can we go one slide further?

This was our response that we presented to the Standards Committee and I don't think any changes were made; am I right Jeremy? I don't think...I think the only comment...the main comment that I heard was the...that first bullet, ONC should work to advance a consistent trust framework across the health IT

ecosystem, and they wanted clarification that that didn't mean that every si...every organization had to implement FISMA, for example but that it really be a trust framework that's compatible across all organizations. Yes? Somebody's saying s...

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

Yeah, that's what I recall, Dixie.

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

Okay. We might want to clarify that in the...make it be advance a compatible trust or something that says that it doesn't have to be the same, does consistent say that?

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

Yeah, I think we can clarify a little here to make the intent more clear.

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

That would be great, thank you.

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

Yup.

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

Okay, let's go to the next slide, which is the frameworks, remember we had the long discussion about frameworks and I think Jeremy's teams done a good job of capturing what we had to say about really learning from the Cyberspace Trustmark, NSTIC Trustmark. We also said...referred them to the CAB-forum Baseline Requirements and to the minimum state of metrics that insurance companies, cybersecurity insurance companies have. I'll give you a second to remind yourself of what we said there. Okay, let's go to the next slide, I think there's...and this is the one about encryption and our recommendations about encryption.

Okay, if you do have any additional comments about those, why don't you just send them in an email to me, that would be fine? And let's go back to...now to section F, which we've discussed and we have draft comments for, but we haven't presented this to the Standards Committee identity and authentication. So this is what ID proofing and authentication standards, policies and protocols can we borrow from? And as you'll recall...and they ask whether healthcare is different from banking and social media and email, and we said yes.

So our draft response is that first ONC along with OCR, other federal partners and industry stakeholders should consider following the NSTIC Program closely and pull from existing pilots where applicable. The NSTIC program has a number of pilots underway and NSTICs purpose, as you'll remember, is really to encourage the use of...the development and use of a set of standards for identity that can be shared across not only organizations, but industry; such as you might take an identity that you got from your bank and be able to use it with your doctor.

Second, ONC should consider providing guidance on the use of third party identity proofing services. This was brought up in the Tiger Team some time ago about how in rural areas it might be necessary to

use post offices, for example, to do identity proofing to give people an ident...third, ONC should work in conjunction with NIST regarding the pending changes in NIST 800-63 version 2. We've brought this up before, and I know that Peter's actually involved in that. Is there anything else we should say there, Peter? Are you still there? Okay, maybe he had to drop off.

Fourth, ONC should endorse the use of trusted Internet identity that may already be used by many individuals for everyday aspects of life, such as shopping, etcetera. What were we saying here...should endorse the use of a trusted identity, like Facebook? Does this say...what's the difference between this and what we said in A or the first? What's the difference between first and the fourth bullets? I guess one is...could we combine those two?

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

Yeah, we can look at doing that.

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

The fourth...

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

The other th...sorry Dixie...

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

(Indiscernible)

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

Sorry Dixie, this is Scott. I was going to suggest that on the fourth one where we talk about using identity that may already be in use, we should perhaps qualify that; it should be...because the last dot point really does qualify that where we talk about a having a higher level of standard that needs to apply to identity for healthcare. So we do want to leverage what's being used for everyday aspects, as long as they meet that criteria of the higher standards.

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

Yeah. Good point, good point. Actually, I think at our last...

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

This is Peter; can you guys hear me now?

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

Yes.

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

Okay, because I was talking before when you called on me, I had to hang up and call back in because nobody could hear me. Sorry about that. Go ahead.

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

Did you have anything to say about 800-63?

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

That I haven't really been inv...I'm supposed to be involved in it, but I haven't really been involved in that for at least a year at this point.

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

Hmm. I don't have any idea where that stands, do you know, Jeremy?

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

I do not know.

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

Is ONC involved in that?

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

I'm not personally. I can check around and see if others are.

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

Yeah, make sure that that's still moving forward so the...

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

Right.

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

So Dixie, this is...

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

...recommend makes sense. Umm hmm, yes.

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

This is Jason. Last I know, it was out, I...the version 2 of it; but the document still doesn't do a good job of telling you how to figure out which level of assurance you need.

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

Yeah, version...

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

It describes what the assurance levels are, but you still need to refer back and it's...designed to be used in the federal space where you have a system categorization and based on that you determine which set of controls you follow under the 800-53 and that points you to whether or not you need multifactor and then you refer to 63 to figure out which version.

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

Yeah. Actually I think this is...we had a presentation, as you'll recall, from NIST that they really are in the midst of revamping 800-63 and getting rid of those levels of assurance entirely and replacing them with the Trustmark; do you recall that presentation?

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

I do, but I haven't seen it yet. But then it's a different version besides the version 2, because I thought version 2 was on...

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

Yeah.

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

...the site.

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

Yeah, I think this bullet is not stated exactly like it should be because there were...NIST is working on replacing 800-63s level of assurance model with these Trustmarks, so it's not really pending changes to version 2, it's really the revamp of 800-63.

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

Okay, but then I still think we have the question, because even if it distinguishes different levels of trust, we still need to figure out how to apply those and we would need standards there, at least some guidance there.

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

Yeah, I think that's a good point. We could...let's capture the idea that we want to...ONC should work in conjunction with NIST regarding the pending changes to 800-63, forget version 2 and to specify explicit applicability to healthcare use cases.

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

Couldn't have said it better myself.

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

Dixie, this is Scott and if I recall correctly, NIST was investigating changing the model and they talked about going to different factors rather than levels and the levels was the confusing bit. And I believe they're investigating, it wasn't necessarily clear to me that they were going to come up with a workable model and it was until they came up with a workable model, they weren't going to be producing a new version of 800-63. But I agree that we should have a voice and participate in that process and then yes, certainly at the end of the day what we really need is then an implementation guide for healthcare as it relates to whatever comes out of that process.

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

Yeah, yeah. Yeah, that's exactly what we need to capture here, yup. I thought that he said they had committed to the Trustmarks, but maybe I misunderstood that. Remember he had all those slides that talked specifically about the Trustmarks, but maybe that was just him talking. I don't know. But yes, we do need an implementation guide for specific healthcare use cases. And I think this last one, although good cybersecurity best practices...this last one is where we say, indeed healthcare is different from these others. I would like to see that come sooner in this list, maybe first, because that's really what they've...I think that that is an essential understanding before we introduce the rest really.

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

Right. Yup, we can do that.

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

I agree.

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

Okay, let's go to the next slide. I'm making a note. Okay, oh, I thought we had another slide for F, I guess that was the end of F. Was that the end of F, that's all it was? It just was one, hmm. Okay; all right, then I think we've been through all of the questions that were asked of us. Jeremy, how does your team...your team will capture our response to G and update...make these few changes to F and then perhaps we can circulate that among the group members?

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

Yup, those will be the next steps.

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

Okay. Now are there any other comments that any of you wanted to make about the roadmap around security, any of the specific recommendations that they made. We sent to you the roadmap sections last week and that roadmap sections...or not last week, right before the last meeting, and that...and it included a number of specific critical actions they call them. And hopefully you've had a...are there any of those critical actions, those actions that they're recommending that you wanted to comment on?

M

Do we have time to bring them up on the presentation and look at them together?

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

Can you do that, Altarum team back there, can you...is that something that's achievable? No, not that, it's the roadmap PDF that was distributed for our last call.

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

It'll take us a few minutes to upload it.

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

Okay.

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

Right Lonnie?

Lonnie Moore – Meetings Coordinator – Altarum Institute

I'm bringing it up right away.

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

Let me see, I have...

Lonnie Moore – Meetings Coordinator – Altarum Institute

Thank you.

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

Thank you.

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

Great. I can start reading you these. The first, E1 was on cybersecurity, it had 5 specific actions; the first was ONC will work with OCR to release an updated security risk assessment tool and hold appropriate educational and outreach programs. I think we would agree with that, we've talked about that before. Two, ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response on priority issues related to cybersecurity for critical public health infrastructure.

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

And Dixie, this is Jeremy; just as reminder for the group, as we're going through and looking at the critical actions, think about not just the action itself, but also the timeframe and is it realistic in the timeframe that we're proposing or will it take longer than we're thinking or shorter than we're thinking. So that's another thing that we're interested in receiving feedback on.

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

That's good, that's good; yes. What I'm reading you are the 2015-2017 timeframe. And then they also ask for stakeholder input on the 2018-2020 and 2021-2024 timeframes. I have this...now, yeah, down...just kind of scroll down on that document, there, that table right there. Can you zoom in? Yeah, now, perfect. Can people...can you zoom a little tiny bit more? Perfect. So the first one was what I read you. Personally I think the second one, it says to cybersecurity for critical public health infrastructure. To me public health is public health, but cybersecurity is just as critical for clinic...you know, clinical health, hospitals and providers as it is for public health.

M

But I think what this is saying is simply that we'll coordinate, that the work being done on the public health infrastructure should be coordinated with the work being done on the clinical health infrastructure.

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

That's not what that says. It says ONC will coordinate with this ASPR on priority issues related to cybersecurity for critical public health infrastructure.

M

Well I guess I would provide the feedback then that what it should say is that we will coordinate work on general health information infrastructure with their work on public health infrastructure.

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

Well I think in general, I mean this preparedness and response is to, for example, to prepare for response. Let's say one of these attackers that we've seen attack Anthem, etcetera, decide that they want to attack the health industry in general, not just these individual places; they want to go out, one fell swoop, they're going out and they're attacking the five major hospitals in the US.

There's no organized way that the healthcare industry can respond to such an attack, in fact, I would say the public health infrastructure is more ready to respond to such an attack because they do communicate with each other, than if the attack were targeted at specific hospitals. Because in the clinical world, there is no concerted...like in ISAC that we've discussed before; there's no concerted communication among hospitals, for example, about attacks that they might have been subject to. So I would say that it's not criti...just critical public health infrastructure, but it's critical health infrastructure.

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

Dixie, this is Jason; I agree with that and I agree with the person that mentioned the expansion of our recommendation before. I think the underlying issue, at least for this next 3-year timeframe is that as we increasingly put all of these clinical records into electronic health records and put them online, when online isn't available, it's going to put a real challenge on our ability to deliver care.

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

Um hmm.

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

I know that there are a couple of systems that FEMA has developed; so for example, when Katrina happened and you had first responders and clinicians delivering care in an emergency situation, they have a need to capture that information recorded, and they have kind of offline systems that work with satellites, for example.

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

Um hmm.

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

But we're not doing that as a nation and I think that's really part of what we need to focus this recommendation on. You're right, it becomes just...it's not just public, it's the entire nation's healthcare ecosystem is becoming critical infrastructure...

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

Absolutely.

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

...and we need to make sure that that's resilient.

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

Perfect, I couldn't have said it better. I tried, but I couldn't. But yes, that's exactly what I'm trying to say. Yup, it's the entire health ecosystem that's becoming more and more vulnerable. Yeah. So can we ca...are you capturing these comments, Jeremy, about that one? Your team?

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

Yes, yup, we'll make sure it gets incorporated.

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

Good, thank you.

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

So if I might, the specific reference, if we have time to look it up offline and I can dig some stuff up if you want, but the system in question is NDMS that's the National Disaster Management System and it's basically an emergency health record that you use in offline situations in crisis mode.

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

Yeah, actually that's exactly the kind of thing I was referring to when I said the public health system is much more...it's much more ready to respond to an attack, any kind of disaster, health disaster, including cyberattacks than the health ecosystem; because they do have systems like that. So, yeah.

Okay, the third one, I can hardly read that, but...the third one is HHS will continue to support, promote and enhance the establishment of a single health and public health cybersecurity Information Sharing and Analysis Center, ISAC, for bidirectional information sharing about cyber threats and vulnerabilities between private healthcare industry and the federal government. Now an ISAC, for those of you who may not know, the ISAC is something, oh they were launched maybe 10 years ago and the financial system probably puts it to best use, but they allow organizations to anonymously report cyberattacks and they disseminate information out to their...about potential cyberattacks, potential threats and recommendations on how to...what to do to avoid them.

And I think that they've been trying to implement a health ISAC for a number of years, I know they have because I've met with the people at least 5 years ago that were trying to do that, but I guess they're putting a more conscious effort toward building...deploying an ISAC for healthcare. I think...maybe Julie, I think it was Julie that mentioned that at one of our meetings. Are there any comments about that?

The fourth one is, ONC will work with NIST and OCR to finalize and publish the NIST Critical Infrastructure Cybersecurity Framework and Health Insurance Portability and Accountability Act, Security Rule crosswalk. Huh. I don't know anything about that. Jeremy, can you explain that...do you know anything about that? I guess it...

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

Yeah, I don't...yeah, I don't have all the details but basically what we're referring to there, so you have the NIST Cybersecurity Framework and the activities described in that framework align with HIPAA and so OCR, being the regulatory body that is responsible for providing guidance around HIPAA compliance, what we're proposing here is working with them to provide guidance around the...how the NIST Cybersecurity Framework could be a vehicle for meeting HIPAA security requirements.

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

Okay, HIPAA security requirements certainly aren't cybersecurity...related to very...I mean, they're more how you implement basically security than really how you respond to an attack or detect a potential attack or, you know, anything like that or between...as we've brought up in this group, between organizations. They're really more focused on enterprises, individual, so I think we'll find some gaps there. The last one here is HHS will work with the industry to develop and propose a uniform approach to enforcing cybersecurity in healthcare in concert with enforcement of HIPAA rules. I guess that's saying much the same thing, how to prepare for cyberattack.

The encryption ones are ONC will work with OCR and industry organizations to develop at rest standards for data encryption and provide technical assistance. OCR will consider whether additional guidance or rulemaking is necessary. Now can you...if you guys can read these, can you scroll down a little bit so they can see all of them on encryption? And maybe zoom in some more, if it's possible? Maybe not...yeah, why don't we read through those and if there are any comments about any of them, or if you have any recommendations for the out years, as Jeremy's pointed out, bring that up. Any comments?

Okay, why don't we go to...let's see, what's the next ones? Scroll down, 2, 3, 4, the next ones are on page 61 and have to do with identity and authentication of participants; there. Okay, you can...yeah, I think you can read those. You know, one of the things that, and it relates to a comment that one of you made a while ago about vulnerability to denial of service attacks. There's really nothing in HIPAA that would protect them against a denial of service attack. Really there's nothing in HIPAA that is geared toward protection against attack, it's more how you implement security within your enterprise.

It would be...it seems like, I guess this is in the cybersecurity space, but there...in the healthcare industry, there's a basic need to address, especially now that health information is currently the number 1 target for attackers; it's become number 1 target and yet there's no real regulatory requirements or industry initiatives that are aimed at really preparing the industry for concerted attacks on...broad attacks on the industry, either denial of service or multiple attacks across multiple organizations.

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

So Dixie, this is Scott. Isn't that what your ISACs are for? The ISACs are the ones that do the coordination of where that's happening across the industry, so you need some mechanism of reporting into the ISAC and being able to share information; that's the purpose of the ISAC. But when it comes to denial of service attacks, then you really need to, I mean the best that I think that we can do at this point is we should be insisting that as part of your cybersecurity position that you need to have prepared and have a mechanism for how do you respond to these types of attacks and be able to action those plans.

And...because it's not a matter of if it's going to happen, it's just a matter of when it's going to happen and so part of your cybersecurity plan should cater for that and you should understand what steps you

plan to take and that you should have a team or at least a process in place that responds when that event occurs.

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

Yeah, and the ability to detect it, they should monitor their, you know, the ports into their organization to detect when there's a concerted attempt to come through, umm, and there's a, what is it...there are certainly tools out there that you can implement to detect potential denial of service attacks.

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

Dixie...

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

There are and it's not just having tools that allow you to detect them, it's usually those type of interfaces into your network are probably going to be controlled by a third party and so whoever your network service provider is, you need to have some agreements in place with them that when you're experiencing some type of things like that that you have ways through coordination with your network services provider of being able to isolate or perhaps inoculate yourself from certain points of attack.

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

Yeah, that's a really good point.

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

So Dixie, this is Jason again. I want to echo everything that Scott said, but I might suggest that we break it up into two different timeframes. I want to go back to the ISACs, right now the ISACs tend to be used where organizations share things too late so other organizations get the benefit, that's good, but it's not really preventative control for the organization doing the sharing.

Now some of the ISACs that are out there, and that's part of the recommendation is to make sure that they're consolidated, but part of the recomme...part of the ISACs that many of the commercial payer side folks use, they share it when they're seeing something that's anomalous and they're saying to the rest of the community, have you seen this before?

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

Um hmm.

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

Because you'll know when you have a denial of service attack; when your folks can't get in and the phones light up, you'll know that you're subject to a DDoS, but long before that, if you're seeing something strange that nobody's seen before, that's when we need them to share it. That I think is part of the first phase, but the second phase, I don't know that there are many organizations, even if they've got great intelligence coming back from an ISAC, I don't know that they're in a position to consume it, right? That's a fairly educated, seasoned, expensive resource or team that they would need. So I think that may be something for an out year phase recommendation.

And then the third point to all of this is that, as Scott mentioned, about the network service providers. One of the unfortunate unintended consequences, at least in the United States of the Divestiture Agreement with AT&T is that the phone companies who are often these ISPs, they have strong cyber practices, but they're not actually allowed to leverage those skills on your behalf because that's considered monopolistic. And I've been through a couple of these real DDoSs where it was our folks on our side that had to craft the filters and feed the ISP what they needed to do to limit the traffic, to keep the bad stuff out and allow our good stuff to trickle back in. They weren't actually able to help us.

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

Huh.

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

That's just one of those lessons learned that only go from having been through it a couple of times. So I would love to see us kind of...question is that, how they could promote standards that would allow, through the ISAC in a non-monopolistic way, where those talents and experiences come that we could all benefit from it.

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

Yeah, yeah. Now I thought ISAC did allow sharing of information regarding a pending...possible pending attack, before it ever happened.

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

Yeah so they do...

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

Oh so they certainly do.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
Yeah, sorry, I was going to say they do but it's all about timeliness, right, and when that....

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

Right.

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

...is there somebody who's actually paying attention to that list, but for instance, I used to participate in a similar forum for Ivy League schools, essentially and so, if one Ivy League school was under a DDoS, then the security engineer at the targeted institution would be sharing directly with their peers, this is what we're seeing, and so that when they...that one particular school shut them down and they turned their attention, the attacker turned the attention to perhaps a different ivy League school they were prepared and knew where it was coming from.

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

Huh, that's...you know, the point that was made about the ability to consume information from the ISAC is a very good one, too. Maybe we could attach that to the ISAC recommendation because one thing is to get this information, but if you don't have any...if you don't have a clue what to do when you get it, or

how to consume it electronically for that matter, it's not going to do you much good because these...a lot of these things are very time critical. That's a good point.

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

Yeah, in the defense sector they've gone through the same thing, just a little earlier than us. USCybercom and the whole defense sector recognize that they didn't have enough security personnel, let alone those that were clear, but folks that were certified and made a huge, enormous effort to try to encourage the industry to get 10,000 cyber professionals stood up in the next couple of years, right? I think we need to do the same thing with the spin that they also need to understand healthcare because again, it's a little different in healthcare.

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

Yeah and you know, when they get the kinds of attack, and I've said this for years, the kinds of attack they've been getting so far have been disclosure attacks. Once they start getting data integrity attacks and service attacks, there will be a critical need to respond very, very quickly. When they have a disclosure attack, yeah, they have to respond but it's not near as safety critical as if you had a data integrity attack or a service...denial of service attack. And I think that they need to somehow prepare themselves for that, because it requires a totally different response.

Hmm. Okay, any other points that...very good points, very, very good points.

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

So one other point, definitely for an out year; this is Jason again. I would love to see, and maybe it's beyond our charge but, the insurance industry is increasingly part of the whole risk calculus...

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

Um hmm.

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

...and if we could get to the point where healthcare organizations through reasonable investments can improve their posture, I would love to see the healthcare insurance companies reduce our premiums on malpractice and other things. To your point, if the network is compromised and the patient data is compromised and we can't trust it, that could lead to failure of delivery of care. If we do this right, we can preclude that from happening and should be able to kind of get the benefit in our pockets.

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

Yeah, yeah. Why is that...would that be in an out year? Why wouldn't...

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

I just think trying to get the entire health insurance...the insurance industry to change, plus, they're...frankly, we've seen the studies that still talk about how many of the small doctor's offices just aren't prepared for HIPAA yet.

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

Yeah.

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

So in order for them to get the reduced premium, they'd have to improve their posture, and that's going to take a while.

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

Actually, that would go very nicely in that 2018-2020, because the objective is expand interoperable health IT and users to improve health and lower cost. So insurance companies giving incentives fits right in to the lowering cost. Yeah, that's a good recommendation.

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

Well, I'm actually guessing if I'm the insurance company, they're not going to lower our premiums, they're going to increase the premiums for those that don't have reasonable posture.

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

Oh yeah, no doubt, it's a money making opportunity. Yeah.

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

As a clinician I would say that may not be true. I did a two hour course last week to get a 5% reduction in my malpractice insurance. They will pay you back if you do stuff that shows that you're reducing your risk. Of course you have to show that you're reducing your risk.

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

Yeah. Okay, I think...let me see. I think the last one is at the bottom there, F2 standards; health IT developers...yup...will leverage existing mobile technologies...I'm not sure what that last one means, does anybody know? Ensure...using RESTful approaches for authentication? Unless they're talking about authorization instead of authentication, you know, maybe they're talking about OAuth 2, but that's authorization, not authentication. I don't know what that means, actually.

Okay, is that all of the recommendations? Let me see, no, there are...there are ones on page 68, if you'll take a look at those quickly, and 69, oh my goodness, there's...I guess these are permission, permission to disclose. These are the consent ones, for section G, yeah.

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

And I would recommend maybe starting down below this one; so the first set of critical actions are more policy-oriented around trying to get better alignment in state regulations that protect patient privacy and impact consent. And so the Privacy & Security Workgroup is commenting on those specific critical actions, so I would scroll down a little bit and focus on...

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

I see, it's on the next page 70, technical.

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

Yeah, I think down below there's a discussion of the actual standards, yeah, here we go, technical standards for basic choice. So, this would be the section that we would love to get your guys feedback on.

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

I think they're...if we have only 5% adoption of interoperable standards for consent by 2020, I will feel like we have failed miserably; but, I've felt that way before.

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

Is there a different target that we should be putting forward here?

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

Adoption has begun...2020, it's 2015 now, I think once we get the standards in place the adoption will come quickly because before we had electronic health records, the signed form worked just fine. But now that we have electronic health records and we're being asked to share them for various purposes, it's really going to become...becoming essential to be able to share them and to know whether they are shareable for...especially for...in the research arena, because that's a movement that's happening really fast with the Precision Medicine Initiative, I think 50, but I...you know, we'll see.

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

Dixie, this is John Hummel. Why wouldn't we want to put that into a tighter timeframe? Because extending that out to 2020, five years from now when we're working so hard to get the HIEs online and get the Blue Button ready to go...

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

Yeah.

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

...to me it seems like it's too far out.

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

Yeah, to me it is, too. Yeah. I think a 5% target...adoption begun with 5% target should be in the 2017 timeframe.

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

Yes, I agree.

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

Okay. And then this individual choice for data provenance...it's interesting that this one has material in the other two columns and I've never seen material in the other two columns on anything else, that's interesting. See on the basic choice they have 2021-2024, technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual basic choice. There's no way that's going to be way out in 2021-2024; I mean for one thing, just the fact that genomic data will be there will force it back to 2018-2020. And information in research,

no, it's happening right now, it's going to be back in...that's what I think. Okay then I think that's it, the data standards.

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

Great. Were there any last minute comments before we see if there were any public comments?

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

I think we're ready.

Public Comments

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

Lonnie, can you please open the lines?

Lonnie Moore – Meetings Coordinator – Altarum Institute

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

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

While we wait for...to hear from the operator, Jeremy, do you want to talk about next steps?

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

Sure, so what the next steps are, so we will work through, compile these comments and get them over to Dixie and Lisa for final review and then we will get them out to the working group members to give them one last read through and make sure that we captured everything accurately and appropriately. And then coming up in the April Standards Committee meeting, we'll present our final recommendations back to the Standards Committee. And then they'll be compiled with the rest of the Standards Committee workgroup recommendations and then they will be come back as formal recommendations back to ONC.

And then as far as our upcoming working group meetings, as I'm sure everyone is aware, ONC and CMS released the 2015 NPRM for the Certification Rule and the MU3 NPRM respectively. And so please start reviewing those because that will be the next thing on our work plan, on our agenda, is to review the privacy and security pieces of the 2015 Certification Rule NPRM and comment on those.

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

Yeah, thank you for bringing that up Jeremy. For those of you who haven't had a chance to look at...to read through or to look at the NPRM Certification, I do have good news to tell you is that ONC took our recommendations almost verbatim. Where we've expressed concern a number of times that beginning in 2014 modules no longer had...were...had to be certified against the security recommendations, the security criteria and standards.

And this working group recommended that the security...that the security requirements be specifically allocated to different types of modules, like a clinical module versus a quality module, for example and we did a mapping, Lisa led this part, we did a mapping that says, okay, this requirement is applicable to clinical and right across the board and that's exactly what's in there. So, I was really, really pleased because not including the security in the module certification really was not fair to providers who had to just sort of guess whether their set of certified modules were going to allow them to confo...comply with HIPAA. So, I was very pleased with that outcome.

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

Well thank you Dixie and Jeremy for that update. Just so you know, there's no public comment. So look forward to future discussions on the NPRM and thank you all.

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

Yeah, thank you all. Bye, bye.

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

Thank you and have a great day.

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

Goodbye everyone.

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

Thanks everyone.