



**HIT Standards Committee
Transport and Security Standards Workgroup
Final Transcript
March 11, 2015**

Presentation

Operator

Thank you, all lines are now bridged.

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

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

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

I'm here.

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

Hi, Dixie. Lisa Gallagher?

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

Here.

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

Hi, Lisa. Aaron Miri?

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

Here.

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

Hi, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief 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.

Here.

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

Hi, Brian.

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

Hi.

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

Jason Taule?

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

I'm here.

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

Hi, Jason. Jeff Brandt? 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 & 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

Sharon...oh, hi Scott. Sharon Terry? And Steven Lane?

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

I am 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 Jeremy Maxwell?

Jeremy Maxwell, PhD – IT Security Specialist – 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

Hi, Jeremy. Any other ONC staff members on the line? Okay, I'll turn it back to you Dixie and Lisa.

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

Okay, thank you. Thanks to everybody for calling in today. It sounds like we have a terrific representation of the working group on our call today and that's great. Today we're going to continue our discussion of the actions and questions that were assigned to the Transport and Security Working Group to review with respect to the ONC's roadmap, interoperability roadmap.

We're going to start by going over a couple of straw responses to the questions that were given us and that we discussed at our last meeting regarding Section E. And hopefully the majority of our...and we do want discussion if you have any problem with these or anything to add to these straw recommendations and then we'll move onto Sections F and G, and the questions that were assigned to us with respect to those sections.

We distributed to all of you a copy of specifically the Sections E, F and G as well as the appendix of the roadmap documentation so it would be easier for you to find exactly the pieces of the roadmap document that we're discussing so hopefully that was useful to you.

Okay, with that let's move on to our questions. Let's see you already have moved on. Section E, as I mentioned, we were specifically assigned Sections E, F and G, and we were asked very specific questions about those standards which is what we're going through.

As time will allow we'll also be discussing the specific recommendations but we wanted to address the questions first and then move on to any further comments that we may want to put forward.

So, at our last meeting we went over the two questions that were or the two areas that we were asked questions about the last time in Section E and those were two questions regarding cybersecurity and one question that was specifically titled encryption.

The cybersecurity questions were what should the federal government specifically focus on first to move to a uniform approach to enforcing cybersecurity in healthcare, keeping HIPAA and the certified electronic health records technology rules in mind and possible new cybersecurity legislation.

The second question in cybersecurity was, are there frameworks, methodologies, incentive programs, etcetera that the healthcare industry has not, but should, consider?

And then the one question we were asked with respect to encryption was, are there other gaps aside from the lack of policies and guidance for implementing encryption in technology and standards for encryption?

We've been asked, as you can see here, we've been asked one question regarding Section F and Section F deals with identity and authentication and one question regarding Section G which focuses on consent.

So, why don't we move onto the next slide and the specific...oh, this is the dates? At our last meeting we discussed Section E, today is Section F and G, by March 25th we are asking you to hold that open for additional discussion and final review of our draft recommendations and for any other topics that may be brought up from time to time as we go through the roadmap. And then the April 6th is the complete comments are due and prepare for submission. They're actually due at the April meeting of the Health Information Technology Standards Committee which is what the 15th?

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

April 22nd.

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

The 22nd that's when they're actually due to be presented to the Standards Committee. So, we do have some extra time there. Okay, next slide, please.

Okay, the focusing in on Section E and these questions that I just read to you, two questions regarding cybersecurity, one question regarding encryption and please show our straw recommendation. Next slide.

Okay, the question about what the federal government should focus on first to move toward this uniform approach to enforcing cybersecurity in healthcare. Our straw response is that our Workgroup believes that ONC should partner with other federal agencies and industry stakeholders in several ways to address a uniform approach to enforcing cybersecurity in healthcare and this straw response, I hope you'll see the key points that we made in our past discussion.

First, ONC should work to advance a consistent trust framework across the health IT ecosystem.

Second, ONC should support the development of consistent accreditation.

Third, ONC should work with industry to advance acknowledgement of the heterogeneity of the infrastructure. This infrastructure must be flexible in that it should permit any certified health IT solution to operate within the ecosystem regardless of what new devices...okay and fourth, let's see, what I see here...is this the latest version? I'm addressing this to the ONC group.

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

I believe so, one second, let me double check.

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

Okay and then fourth the ONC should provide guidance on proper governance in cybersecurity which is essential for building trust and security throughout the ecosystem.

And then finally, the ONC should bring together federal, state and industry stakeholders to address the goal of reducing variations in cybersecurity enforcement. And yeah, I do think this is the latest one. I was misreading one of them.

Okay, let's have...if you have discussion...and Lisa do you want to add anything about our response or a question here?

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

No, I think I'd like to hear from the Workgroup members.

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

Okay.

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

So, yeah, let's open it for discussion.

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

Were...

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

So, Dixie?

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

Yeah...

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

Dixie, this is Steven Lane, I have a question under the third item because I'm just not quite sure what the wording means. When we say that we believe that the ONC should work with industry to advance acknowledgment of the heterogeneity of infrastructure what does that mean when we say...

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

That's where I...

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

To advance acknowledgment?

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

Yeah, that's where I tripped up too, I didn't think that our final version said that, but apparently it did, let me see.

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

Dixie, do you want me to elaborate? I think there was a comment there, I'm Aaron Miri by the way, I believe the comment was last time we were focusing in on the mobile aspect, you were saying mobile phone in the interoperability or the map and I believe what we were trying to get across was that it should be across platforms not so specific to say phones, but it could be anything hence the heterogeneity, now I agree that's sort of a very complex sentence but I believe the concept was it needs to be ubiquitous, it needs to be just across the entire playing field.

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

Yeah, I think...

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

Do we...

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

Both of us tripped over the term "advance acknowledgment" which maybe we could come up with a better way to say that, should acknowledge I think it should be maybe.

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

Well, is it acknowledge or accommodate? I mean, do we...we want to actually deal with this heterogeneity, right?

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

Yeah, not just to say that it's there.

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

Yes.

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

Yeah, I think that would be good, yeah, accommodate the heterogeneity I like that, that sounds good.

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

Yeah and this isn't saying much for all these words here, and this is Peter for those who don't recognize my voice, it doesn't say much, it's very, very generic and I think that we probably want to say a little bit more and stick our necks out a little on it. I like the point about, you know, acknowledge...what was the word you used for the heterogeneity?

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

Accommodate.

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

Accommodate.

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

Accommodate, you don't want to just acknowledge it, we want to move towards it and maybe we should mention, you know, to support the work of the IDESG or something of that nature that would, you know, say we realize this is going to need to be a federated system and let's start working that way because it's not going to be...it's going to be too big to be centralized. What we're saying here I think people could read almost anything they want into it.

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

Well, I personally hate the word "federated" because it's so misused these days, you know, federated...

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

When I use it I'm using it the way that you're thinking of it from a few years ago, if there is another word that's replaced it that's not misused let's use that.

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

Yeah, interoperability is better I think...you know, federated databases are quite complex for example. Federated identity is not. I think people misuse that term a lot. So, I in particular would not like to use it here because it's gotten so it has no meaning at all. But if we said accommodate the heterogeneity of infrastructure must be...

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

Do we want to mention any groups that are working on it like the NSTIC groups?

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

Well, I don't think they are except for the identity piece of it.

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

Right.

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

I think what...the discussion was not specifically about identity it was really about how we really need to be able to build a secure infrastructure despite the fact that we have mobile and we have, you know, we no longer have boundaries around organizations, you know, there is a very heterogeneity...and we have different EHRs, the cloud.

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

Right, that's exactly right, Dixie, this is Aaron, again, as a comment specifically, and I know it because I'm the one who raised my hand on it first, was that what alarms me is when we start saying a specific form factor to use in this case, mobile phones, I said, now you're limiting the innovation of the market, you know, we should be acknowledging technology absolutely but it should be across the entire landscape. So, to what Dixie is saying, I think the emphasis of this Workgroup is, hey let's not pigeonhole ourselves before we even get started.

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

I think we need...

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

I wasn't trying to pigeonhole us and I wasn't trying to specify the device I was just trying to specify a process but I'm fine with that as long as we talk about accommodating it that's good. Maybe we want to put that at the top or in bold so that people realize that that's the meat of the statement.

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

Yeah, I think, this is Lisa, I think that the wording is...you know there are probably ways we could make it a little clearer as to our meaning and Dixie I know you will explain this when you're giving the presentation but we may want it to stand alone. Aaron, do you have any suggestions that would, you know, clarifying as to the intent?

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

Yeah, I think, again, accommodate is the right word versus acknowledge. And, you know, when you say heterogeneity as a CIO I read that and I'm like, what the heck does that mean? As a technologist I understand, okay, you mean across all different domains.

So, the intent again is that we want a level playing field on every aspect that is secure that can leverage all types of methodologies again to allow innovation, allow the marketplace to dictate, you know, the course of where this goes.

So to the degree of it, you know, I'm definitely not a wordsmith in the least but accommodate is the right word. Heterogeneity I'm not sure.

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

The part that...I like accommodate, the part that still gives me grief when I read it out loud is, now, is the regardless of what new devices or service delivery models are added, you know, that's just not realistic.

There are devices out there that we really don't want used in healthcare and delivery...I don't think we mean regardless, I think we mean, you know, it still has to be secured, it has to be...well, I misused the word there, but it still has to be trustworthy shall we say.

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

What if we...Dixie, let me ask you this, what if we tie in, and this goes back to the earlier comment, something about NIST or something around, you know, that leverage the standards set forth in the NIST, you know, NIST publications or whatever so at least we give it some level of depth that we're talking about devices that meet specification not something built in someone's garage.

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

Well, we could put...we could put a reference to NIST in the first sentence, you know, the...

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

Yeah, there you go, I mean, something to give it some credibility and some meat, I mean, again, I'm going back to somebody else's comment there.

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

Yes.

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

And I think we tie it back to something like NIST which is a very credible source and becoming even more credible if that's possible, that, you know, we at least show that we're trying to tie this back, but still allow a level playing field.

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

Okay, if we mention NIST does that mean we need to mention other federal agencies?

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

Well, I think when we're referring to guidance and standards it's okay to, you know, use...

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

Okay.

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

NIST as a sole example to me, this is Lisa.

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

Why don't we say partner with NIST and other federal agencies?

M

That's good, Lisa.

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

It sounds good.

M

Yes.

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

Yeah, I was on mute, sorry, Dixie, yeah that's great.

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

Okay. Is there any...so we've got two changes to that. The accommodate and NIST and other federal agencies. Are there other changes, things that we didn't capture from last discussion?

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

Well the other comment, Dixie that we had talked about was the importance and it might not be this section, but the importance of working with other agencies like the OCR and others to sort of have that cohesive collaboration moving forward, right?

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

Yes.

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

So, that there wasn't any potential for misperception but I don't know if that's appropriate for this question, but that was the other big topic we focused on.

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

Well, this is where it would go I think because the other one...let me see I think I have it open here.

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

Yeah, because one of the items that...well not one of, but, you know, a major bullet point that even...that HIMSS put forth last year and in the Health IT week was the need for a roadmap and the need for the agencies to work together and they are, I think there is just opportunity to further drive, you know, any chance of misperception out of the water by putting things like work together with OCR and, you know, anybody else as appropriate to collaboratively drive this to goal and I think that will show that throughout all aspects of this roadmap and going forward that we're always thinking about the inclusive of all.

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

So, do you think that we should explicitly mention OCR?

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

As a healthcare CIO, yes, because that's obviously on my radar a lot to make sure that we're complying with everything and they don't knock on my door for the wrong reason. But, I don't want to speak for the industry. I'm sure there are other agencies too, FDA, whatever, as appropriate that need to be mentioned.

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

So, do you think we should say, NIST, OCR and other federal...I mean, you know, there are lots of...

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

Who is OCR?

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

Office of Civil Rights.

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

Office of Civil Rights. They're the ones who come enforce if you say breach patient data, whatever, they're the ones that come after you and want to look into things, rightfully.

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

They're the HIPAA regulators...

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

Right, rightfully, right, exactly.

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

Okay.

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

And this question.

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

Thanks a lot, sorry to interrupt you Dixie.

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

Yeah, this question is about enforcing so I do think it would be appropriate actually, first to move towards a uniform approach to enforcing cybersecurity.

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

Yes.

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

So, actually it's very, very applicable.

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

Yes.

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

So, why don't we add that as well, okay? Okay, that's a very good point. Okay, can we go to the next slide?

And this one, are there frameworks, methodologies, incentive programs, etcetera, that the healthcare industry has not but should consider?

Our straw response is trust is integral in building a secret...a secure health IT ecosystem. The National Strategy for Trusted Identities in Cyberspace, NSTIC, the IDESG Trustmark should be considered as a possible framework to establish electronic trust between trust frameworks across the Internet.

Additionally, the existing security control frameworks including NIST cybersecurity framework should be considered for alignment and guidance when gaps occur.

Now did we always have IDESG in there? Because I don't think that's necessary.

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

Do you mean NSTIC isn't necessary to mention?

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

NSTIC is sufficient I think.

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

Yeah, the IDESG is just the governing body under NSTIC.

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

Yeah.

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

So, I mean, whatever terminology I think that's fine.

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

Yeah, I think it would be better to leave IDESG, especially since we're not defining it and it's a governance organization, but the NSTIC initiative is coming up with this, across multiple segments of it, is coming up with this Trustmark, also they're working with NIST on that Trustmark.

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

That's right, actually, this is Lisa, you're being precisely correct there. So, I think that's right.

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

Okay. And NIST cybersecurity framework is that the Trustmark?

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

No that's a generic security framework for, you know, implementing security in an organization and there are, you know, several of those out there.

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

Okay.

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

Let me ask this question, is it worth, and this is Aaron, let me ask this question and I'm putting it out there not as a recommendation but more of a question for this group, is it worth us also mentioning other frameworks that are just as important like say PCI or, you know, I don't know SOCs or anything else.

I know it's not necessarily cybersecurity but it is data to some degree whether it's financial or whatever else and at some point or another there has got to be an overlap here that I'm not sure NIST by itself just covers. So, I'm just throwing it on the table as a consideration, do we need to go down that path or stay away from it?

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

Well even...

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

Well this...

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

Even ISO.

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

This is Lisa, I mean; I do think PCI is a good candidate if we want to go in that direction because it really at this point is the only, you know, security framework against which hospitals or healthcare organizations actually get audited for security from time to time.

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

Right.

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

You know we don't have the HIPAA audit program up and running yet, but they do occasionally get a PCI audit and it is kind of...that does show the overlap and it is active. So, you make a good point.

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

Yes.

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

There is also...this is Jason, there is also the HITRUST common security framework method and the advantage to that is that I think it accommodates the fact that the healthcare industry isn't a one-size fits all, it's very different to be a large academic medical hospital versus a small doc-in-the-box, versus a payer, versus a vendor that support covered entities, right?

And I think one of the challenges with NIST is the framework is pretty good by itself but NIST obviously points to all of the NIST special publications in the 800 series and candidly I think there are very few commercial organizations that have the financial wherewithal to begin complying with them and if the purpose of this framework is to kind of support interoperability we all need to be moving towards it or it's not going to do us much good.

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

Well, shouldn't...most private organizations also get ISO 2700 audits. Should that also...I mean, that's probably the security framework to...you know, the most internationally used of all of them.

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

ISO is a very fair one, I mean, and if you wanted to ratchet up you could even mention SSA...or whatever else, I mean, this could be very prescriptive but then we go back to even the earlier point of if we get too prescriptive suddenly you eliminate the ability for innovation or you mitigate it you don't eliminate it, you mitigate the ability for there being any type of innovation in the marketplace.

So, stuff like NIST and others are generally referenceable and tend to be followed. HITRUST, and I've gone down the HITRUST path myself and being a CSF organization, is a great framework but it is also very difficult to achieve, so just a level of prescription.

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

And what...

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

So, this is Jason again, if I might suggest, for all of these things I think there's a difference between a minimum baseline of table stakes that we all want from one another but also to the previous point not being so prescriptive that it forces us to operate a single way. But for the industry to move forward I do think for that bottom minimum we do want to be a little more specific so that we all know what that looks like.

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

Well, a framework is never that specific, you know, a framework is something that you, you know, you add specifics to, that specifics fit within, you know, it...

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

Dixie...

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

Offers...

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

Sorry.

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

Options. Yeah?

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

Sorry, Dixie, this is Scott and to truly answer the question at hand I don't know that I necessarily have in my mind the list of incentive programs, methodology or frameworks that have already been considered.

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

Yeah.

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

And so we're supposed to be coming up the list that haven't been considered it's a bit hard to do that unless we know what has been considered and some of the things that we've mentioned I think probably fit under the umbrella of having already been considered.

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

That's a good point, I mean, the only incentive program I know of is the, you know, EHR incentive program, are there...

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

Well, I would also say that there is also the incentive not to get audited by following certain frameworks, right?

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

Yes.

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

Now obviously you followed NIST standard, you know, type for levels of encryption and those sorts of things, you know, regarding just HIPAA compliance, so to the degree of it I think there is some referenceable material not necessarily a definitive but there is referenceable material.

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

Yeah and if we thought of the term, instead of incentive if we thought of the term as leverage what leverage, what's leverageable.

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

Yeah.

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

Then we would have a broader set of things that we could consider, this is Lisa, by the way.

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

Yeah that's what they use in the policy side what levers does the government have, I think that's probably what they're talking about, yeah.

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

And incentives there is one type of lever but there are others.

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

Now to me and I know I've brought this up until I've got bruises on my head, but to me one of the principle disincentives if anything is the fact that they don't certify security in EHRs, you know, unless...they will certify security if the vendor asks them to but they don't if the vendor doesn't ask them to and even when they do they don't do...they just do conformance testing they don't do any kind of penetration testing at all or any kind of real security testing.

So, I think that, you know, I think it's an issue that when you buy EHR products you don't know specifically how much security they give you and I think, you know, that's another...it's not really a disincentive but it's a hole in the framework I think.

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

Yeah, so I can say, Dixie, this is Scott again, I can say that if an EHR was acting as a HISP under the DirectTrust framework then there is a security evaluation aspect to that, but, you know, then not the HISP and the EHR are not necessarily comparable entities.

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

Yeah. Well, maybe we could say...that's probably the only place, only entity I know of or only process I know of out there to really get your security certified in healthcare.

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

Well, HITRUST I guess you could consider that also, HITRUST CSF and then of course in the State of Texas there is Secure Texas which is more of a statewide, more privacy focused certification, those are actual certifications that you get that you have to have audited by a third-party that certifies it and all sorts of things. So, there are levels I think...and other private groups out there that do the same thing, but something that is nationally a federally recognized I agree that it is going to be difficult finding one.

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

Yeah and HITRUST is not open, is not an open thing it's a...it's private.

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

That's exactly right, yeah, you pay into it, you're absolutely right, but I'm just saying from a certification perspective you're looking at an open one, yeah, I don't know of many, I wish there were more and I think that's a great opportunity.

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

The HITRUST framework is open, you have to pay an auditor to audit you, but that's true of any audit.

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

And you have to pay HITRUST a fee to participate.

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

Yeah, even to get the standard, the documents, yeah.

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

That changed.

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

Pardon?

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

That changed you don't have to pay to get the common security framework that was part of the criticism when they were a private organization but they switched to non-profit and you can get the framework.

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

The last time I tried to get it I couldn't get it.

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

I'm not sure you can go into the tool, the online tool and submit to HITRUST but I don't want this call to be about HITRUST, I just...

John Travis, FHFMA, CPA – Vice President & Regulatory Solution Strategist – Cerner Corporation

Right.

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

I think there are other frameworks that are more referenceable not that it's a bad framework, it's great, I'm just saying from something like open, like NIST or whatever it's not bad.

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

Yeah.

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

So, going back to this question it's almost a bit troubling in that it doesn't narrowly define what is it that they're questioning we should recommend frameworks to consider for, right? Because depending on what the purpose is, you know, we may or may not think HITRUST is appropriate or any of these others are appropriate either.

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

I think we should capture this point that we moved rapidly past is I think Scott mentioned the lack of really mechanisms for getting your cybersecurity accredited and that HISP is the only one out there.

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

So, to me I think it breaks, again this is Jason, I think it breaks down into two questions, one is a framework so that we can establish levels of trust in one another and then two when we actually need to interconnect with one another what that looks like one would be more esoteric and one would be more bit level specific. Because we don't all want individual one off interconnection standards we want there to be something we can all jointly move towards.

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

So, this question isn't about interconnection standards. This is about cybersecurity for the healthcare industry.

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

Right and for that to happen, for us to be able to exchange data with one another, again this is the Transport and Security Workgroup, right, we need to have trust in one another and when it comes time to actually do that exchange there needs to be mechanisms that facilitate that.

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

Yeah and the only one that accredits that trust for that exchange is the HISP, right, is the...DirectTrust. Is that what you're saying?

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

No, I was saying we might want to frame our response to say, depending on what it is that they're asking us to make a recommendation for, should they consider a framework for this versus that we might want to just caveat that, that was all.

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

So, we should say that it's not clear whether you're talking about a framework for an individual entity or a framework for interconnections?

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

Right, we can make presumptions about that and I was just offering that in my mind it's for those two purposes, one trust and two actual interconnection.

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

Yeah, I see, I think that that's worthy of...yeah, I think that's a really good point.

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

That's a very fair point, this is Aaron, I like that, that's a good perspective.

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

Yeah.

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

You know the other thing I think that we've talked about here that and it might be worth putting out there and I, you know, give credit to the ONC as they're trying to tackle this from multiple directions, you know, is sort of a level set playing field by applying some sort of universal test or litmus test to the environment to say, where is everybody, how is everybody doing, you know, because here we are trying to establish this baseline of what is the appropriate level of security, cybersecurity and I'm not sure we even have an idea of how the ecosystem is doing.

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

Oh, yeah.

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

I mean, so is there...is there some sort of universal, you know, are you 128 bit encrypted at least, are you using SSL, are you encrypting all the devices, data at REST, I mean, is there a standard test that could be applied across the landscape so we at least know then how far to push it because, you know, learning from Meaningful Use we want to make sure that kind of understand, seek first to understand, before we go out there and say, this is the right path and then have to modify an approach later one.

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

Yeah that's a good point that there really is no, other than HIPAA, there is no real metrics for determining, you know, how strong your cybersecurity is and even HIPAA is more of a...at least how it's interpreted is more of a check list kind of thing it's not really a test as to how strong your cybersecurity is.

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

Well, we do have plenty of anecdotal information about how good the industry is just read the headlines every week.

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

Yeah that's right.

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

How did Aetna get away with refusing an audit after they had that breach?

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

So, the last comment, should we capture that there is a need for metrics for measuring how strong security is?

M

Or at least referencing to a standard like the ISO 27001.

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

Yeah, something but even that, you know, I'm thinking about the rural hospital, this is Aaron again, sorry, I'm trying to put my CIO hat on here and say, you know, if I don't know what ISO 27001 is or I don't have the funding to do that what are my bare minimums I have to do at least make sure that I'm doing the right things and I'm not going to be, you know, grossly negligent, encrypt all devices at a certain, you know, level of encryption, you know, not just use some open source whatever out there, you know, I mean there are certain...there could be generally agreed upon universal principles that this should do.

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

Yeah, like...

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

If you reference something, some big arbitrary nebulous thing I might not have the funding to do that and I might be deficient before I even start.

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

So, this is Jason again, I think if OCR were to opine they would suggest that the HIPAA rules do just that with required minimum and addressable, right, I think, part of what we may need is to make a recommendation that there is still unfortunately some question in different organization's mind as to whether or not they're even subject to HIPAA.

I encounter that all the time when I deal with vendors who are absolutely business associates with whom we exchange PHI who don't believe they're associates and don't believe they should have to comply with HIPAA which really makes it hard for me to work with them.

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

Yeah and HIPAA really is very enterprise focused, it's not...you know, going back to the earlier comment about the need to pay attention to the interconnections it's really not interconnection focused in the least it's very enterprise focused.

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

Right but to Aaron's point if they are not yet encrypting data on computer end points for example, which is something we all know we're supposed to be doing it would be very difficult for me to justify a decision to partner with them.

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

Yeah, I like the idea of generally accepted principles because there are lots...I mean, people today don't even...even though the regulations and the guidance is out there people don't even routinely do full disc encryption of laptops, you know, they don't...we're still having those same kinds of, you know, movable device type breaches that really those are generally accepted principles that everybody should...maybe the OCR could develop such generally accepted principles, I bet they know what they are.

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

Dixie, this is Lisa, I would almost term that as minimum standards in certain control areas because that's what people ask me for a lot, you know, it's not a principle it's, you know, at a minimum right now, today you should be doing, you know, x-type of encryption, you should be doing the following this the minimum standard for some of these control areas. Because I think that's what we're asking for and that's where I think a lot of healthcare organizations struggle because they're like we don't know what's good enough, we don't know what we should be doing for our organization.

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

Yes.

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

Even though HIPAA allows us the flexibility to determine that based on our risk assessment we just don't know what that is.

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

That's a very good point.

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

...penetration testing. I mean, I think that's a huge gap but most organizations, you know, they don't do, you know, independent penetration testing of their organizations.

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

Or just say penetration testing in general because if I don't have the funding to go pay a third-party to do it fine I myself as a CIO should take the responsibility on my shoulders to take random phone calls of the medical staff going, hey, you know, this is the IT department give me your help desk or give me your password, user password, you know, just random things like that, you know, that are bare minimum that just...

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

Yeah.

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

Takes time and effort. There is a level of standard, I agree, minimum necessary that really needs to be defined and enforced.

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

Yeah...

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

Well, perhaps one of the things you can do is reference it as minimum knowledge levels because I'm a rural hospital and I just went out and got certified as an ethical hacker so I could do my own pen test because I couldn't get the funding to do an outside pen test.

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

Exactly, exactly my point.

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

Yeah, that's...yeah, good point, yeah, good.

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

Yeah in the absence of money, which is a very real thing today in healthcare, here I'm a healthcare CIO I can tell you directly and every dollar is debating buying a brand new bed or buying, you know, a computer and you know which one wins out 9 times out of 10. I have to do things on my own shoulder, fine, well what you can do is turn on encryption, turn on...do social engineering yourself, you know, those kinds of things.

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

Yeah that's a very, a very, very valid point, yeah.

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

So, if we wanted to, sorry, Dixie, this is Scott again, if we wanted to have a great starting point for those types of things you know back in 2011 the commercial certification authority industry got quite a few hits where, you know, several of the CAs were compromised. In response to that CAB Forum came out which, you know, they set the EV standard for eCommerce, on-line commerce. They came out with some great documentation around network and security controls that are mandatory now for anybody who gets a web trust audit and they cover a lot of, probably all the principles that we've just been talking about that organizations should consider when they are trying to protect their data assets and networks from any type of malicious activity. It's a great document to start with and maybe that's one that we should add to the list.

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

Yeah, what is...I'm not even...CAB Forum?

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

Yeah, CAB Forum it's the CA and browser Forum.

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

CA and browser forum and it's open?

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

But those details are available at cabforum.org.

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

Okay, that's good to know.

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

They're the ones who created the EV standard for SSL certificates.

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

Yeah, that does sound like something we should mention and it's open?

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

Dixie, this is Jason again, Scott made me think of an interesting point, I know we're trying to narrow our discussion here to what we're going to be putting in the deck, but another way of kind of getting at minimum without a strong hammer of enforcement, most of the insurance companies that offer cyber liability products they expect a certain...certainly the questionnaires and the applications that they have us fill out, they ask a certain number of questions and implied in those questions is that you are doing those things. So, we might also look at it from that perspective because then not only is it facilitating interoperability and trust but it's actually buying them something, right? They're able to get insurance, they're able to do it at a less risky premium, etcetera, I think there is real benefit to coming at it from that approach.

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

That's a...

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

It's not just an academic exercise.

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

Yeah, yeah to look...is that pretty standard, all the insurance companies that offer cybersecurity insurance do they ask the same sorts of questions.

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

I don't know that there is an industry body, I suspect if we did a little search we could probably find out, but I've worked with three or four different companies and they all basically ask the exact same questions.

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

Oh, that's a good point. Okay.

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

The things that we've been talking about, are your hard drives encrypted, if you have PHI and you allow it on end points are they encrypted and if you're exchanging it do you have a VPN for remote access it's those kinds of questions.

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

This is John again and as part of our yearly audit for the board we get those same questions asked by our auditors, because it puts the hospital at risk if you do have a cyber-event and you haven't done those steps that you said you did.

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

So, those auditors that you're talking about are auditing for what? You mean like financial auditors and they ask the same questions or are they security auditors, or what kind of auditors are they?

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

It's part of the financial review that we owe to the...because we're a public district, so they bring in auditors each year, they go through, they basically say, you know, where are your risk points and as part of the financial review for potential risk are you meeting or exceeding all your expected HIPAA norms to avoid a fine.

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

So, they actually ask basically the same questions as the insurance companies?

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

Yes.

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

That's interesting. So, that should be pretty easy for, you know, ONC to put together or whomever is responsible for doing that, OCR whatever.

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

One last...

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

Risk...

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

This is Jason again, one last source, I presume most of us are familiar with ISACA, the Information Systems Audit and Control Association, they have an IT Governance Institute and a number of years back they prepared what they called survival kits and it was a series of questions that each of different levels of management should be prepared to have answers to at all times including executives and boards, and for the board level it's 17 questions of almost this exact same conversation, you know, do you know where your data is and what kind of controls is it secured by, etcetera.

So, again they're really good sources for a lot of these, again, not full extensive frameworks, not 500 controls like NIST 800-53 but rather going to that minimum baseline there are some really good useful things to make sure everybody has the minimum in place.

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

Well, I know that that's exactly the kind of thing that ONC is looking for here. So, that's really, really useful. So, we've gotten several sources for those exact kind of minimum standards, good, very good, for control areas, very good. Okay, we'll try to capture all of these and distribute them back out to you, probably by, let me see, we have a third question I think. Let's go to the next question on encryption.

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

Dixie?

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

Yes.

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

This is Lisa, one more point on the previous item.

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

Okay.

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

I know that we said we wanted to recommend that ONC or OCR do this but I know that OCR has been really reluctant to specify minimum standards related to HIPAA and so I don't know if we could, you know, think about some other way to recommend that it moves forward and maybe it is ONC but I don't think there is a likelihood that OCR will do that. Just an FYI. I mean, it's just something I wanted to add that's all.

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

But...this is Aaron, can I just say this and I'm just going to say this and I know...I'm trying to say it as very just openly but it's important, if we don't have the federal agencies at least working together and say it's sanctioned by or in support of or whatever it's going to be very hard for me as a CIO to know that, okay if I do A, B and C that everybody recognizes A, B and C as having weight. If ONC did it in a vacuum or the GAO did it in a vacuum or whoever did it in a vacuum then it would be very tough for me to go justify the dollars necessary to make the minimum standards. So, I'm just putting it...

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

No, I...

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

On the table that it's important for me to see that.

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

I totally agree, I'm just...I think the reality is that because it's HIPAA and they're the regulator they're not going to define...I mean, the whole point of the HIPAA security rule was to not define minimum standards. So, we need some other mechanism to do it. I totally agree with you though it's just that's...I'm just giving background on what I think the reality is from OCR's perspective.

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

And I think this kind of guidance would come out of ONC working with OCR.

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

OCR...

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

Because ONC has that in their charter for publishing...

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

Right.

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

The kind of guidelines.

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

Okay, thanks.

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

That is really good input, I'm sure that this is exactly the kind of thing they're looking for. So, thank you, all. Okay, going to the...

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

Hey, Lisa?

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

I'm sorry?

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

Lisa, this is Jeff Brandt, sorry I was on the other line and I couldn't get through, I don't know if you have seen this but when we were talking about social hacking and PCs and all this stuff that is the easy stuff to take care of, which is also the most difficult, you know, when we did the mHIMSS roadmap I covered a lot of that in there and also then did it in my books that we wrote there is a lot of information there about taking care of that checklist.

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

Yeah, that's true we should probably...Jeff let's get off line and do some homework and pull that out and, you know, take a look at it.

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

Sure.

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

Thanks.

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

Yeah, I think it would be a good idea, you bet.

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

Okay, thank you, thank you Jeff. Okay, I'm making my notes. Okay, encryption, are there other gaps, aside from the lack of policies and guidance for implementing encryption in technology and standards for encryption?

Our straw response is that ONC should work with federal partners and industry stakeholders to address the following three issues related to technology and standards for encryption. First, ONC should provide guidance on key lifecycle management. Second, ONC should provide guidance on a method for key escrow recovery and finally, ONC should publish guidance on key oversight and authorization addressing the people or entities that maintain access to keys.

We should...Jeremy, we should put ONC, let me see, following...somewhere we should put encryption key not key, so it's not misread.

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

Right, yes.

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

Okay because it's easy to just, you know, people use the term key to mean primary as well. So, are there...I mean, basically what we're saying here is they need to address not just the encryption algorithm and the length of the key but the overall environment for encryption and management of encryption keys as well.

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

This is Aaron, I would agree although I think beyond just keys it's just again insuring that the same rules apply for everybody, right?

So, from the perspective of there are medical devices out there that are on the market that we were looking at purchasing as a hospital and when I asked...when we did our risk assessment they didn't even...they were browser-based and they did everything via HTTP and I'm like, you've got to be kidding me guys, you're selling a product which people are buying that you don't even...I mean, it's not even HTTPS which to me is basic 101 stuff.

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

Yeah.

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

So, to the degree of it I think it's just a level of, again, a standard playing field. So, beyond keys just a general, again minimum need, minimum use.

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

It's really, what you're saying I think is that we need the same thing for this one as we had the same thing for...as for the last one, we need a defined set of minimum requirements.

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

Yes, Ma'am.

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

That's a good point and a lot of that is in the PCI standards too. Are there other comments about this one?

Okay, why don't we update these three straw responses to E because this is a lot of...these are a lot of changes and perhaps distribute them by e-mail, but I think we'll want to go over them again at the next meeting anyway because we've made some significant changes here.

So, why don't we go onto the next...we can work with the ONC team to figure out exactly how to work that. Why don't we go to the next question and I think we're starting on Section F.

Section F focuses on identity and authentication and they only ask us...they ask us two questions really, what ID proofing and authentication standards, policies and protocols can we borrow from other industries?

And the second one is healthcare that different from banking, social media or e-mail? The e-mail thing is out of place there, it doesn't...banking and...yeah. Banking seems out of place actually.

Okay, are there...let's begin discussing this one. What ID proofing and authentication standards, policies and protocols can we borrow from other industries?

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

I'd say banking; I would immediately go towards banking. I mean, I see healthcare following the same standards that banking did, again two-factor authentication, the level of certifications, levels of, again, compliance, key management, I mean, the whole nine yards. So, I mean, I look at that...

M

Well, I don't know, I mean banking...

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

Dixie...

M

A lot of banking goes on without multifactor authentication, I mean, I think...

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

And without identity proofing.

M

Yeah.

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

That's correct.

M

I think banking may not be the right term. I mean, real estate transactions come to mind as ones that seem to require a higher, you know, level of identity proofing but I agree I don't think banking, social media or e-mail gets us to the level that we want to pursue in healthcare.

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

And Dixie...

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

Well, banking does have...banking has identity proofing for...

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

Yes.

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

To get an account.

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

I just got...okay, so they don't do identity proofing the way that...they do knowledge-based identity proofing there is no...there are whole accounts you can set up without appearing in person anywhere. So, it's not...

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

Well, it's also...sorry.

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

I have an account on Ally Bank because I went through the process to see what they did it's all knowledge-based identity proofing, it is not in person identity proofing, they never see you, there are no branches but they identity proof you that way. So, that model is changing.

And also Dixie I wanted to add that on the NSTIC pilot that was done on the healthcare organizations they're actually...because I know in Virginia they're looking at the use of third-party identity proofed credentials and the fact that if they can legitimately use those...so they worked with the Virginia Department of Motor Vehicles to get an identity proofed credential from them that they could use as part of the patients, you know, multifactor identity...that they would stop doing the in person identity proofing themselves.

So, the model is moving towards the, you know, sort of the NSTIC kind of identity and if you need an identity proofing get to level 3 or whatever that there perhaps is the ability to use third-party credentials and so we have to be really careful that we accommodate innovation and it's not really another industry but more that eCommerce ecosystem that NSTIC is trying to evolve and this is Lisa by the way.

M

So...

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

So, if you're saying the model is moving toward the use of these third-party identity proofing the model, what do you mean the healthcare or the banking, or just in general?

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

No, I'm saying that is being considered in some of the pilots on the NSTIC program.

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

Okay.

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

And one of the pilots that did that is a healthcare, a hospital system that said, hey, if this works, if we can get, you know, a level 3 identity proofed credential from some other provider like a motor vehicle or whatever we could use it and if we can use it, it does increase security but also it could save millions of dollars in sort of reducing the administrative burden of identity proofing in the ER or on admissions, or whatever you don't have to do that anymore.

So, it is...when I say the model it is the model for the ecosystem and the model for a multifactor, multilevel assurance credential which could include, you know, identity proofed credentials as well and that is something that could be leveraged in healthcare and INOVA went ahead to try to do that and they liked it.

So, you know, it's just a question of, you know, can we have...we need to get third-party credentials up to level 3 and things like that, but, you know, there is definitely a few that how we do identity proofing is going to evolve leveraging technology and so it's not really looking at other sectors but other sectors will definitely use it, banking will use it and others will use it once the ecosystem is adequately evolved which is probably a year or two out at the most.

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

Well, I think that most of what's happening in this whole identity space is being driven by, one way or another, is being driven by NSTIC.

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

Yeah, but, you know, NIST is the sponsor, right, Department of Commerce, NIST, and so they're taking a good look at mapping it to levels of assurance and, you know, allowing each industry to determine what they need for each type of transaction.

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

Right, right, right but I meant that's kind of the...

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

Yes.

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

It's a central piece of it, because each industry is then interpreting...

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

Correct.

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

What NIST is trying to do for its own industry.

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

Correct, yes, so I would say that opposed to looking at banking as you're doing today, we look at NSTIC and see what the possibilities are of how technology can be leveraged in this way.

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

Yeah, look at how other industries are implementing the NSTIC type of...the NSTIC model really.

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

Well and they may not be yet but they will be in the next, you know...because you look at the pilots and that will help give an indication of what they're looking at doing and including healthcare because we had a healthcare pilot that did substantial work on this.

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

Yeah and I understand that Kaiser is involved in NSTIC now too.

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

Yeah, I mean, it's...so I think the whole point is that we need to rephrase the question. I mean...so that we're clear and informative on what's going on, you know, there is new technologies that are going to solve some of this within an ecosystem that's being defined for the nation.

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

Yeah, yeah, yeah so if we were to...yeah and maybe we even make that point at the beginning that what NSTIC is doing, and it's even international at this point, what the NSTIC program is doing is being picked up and carried forward by different industries so what they should look at is how different industries and the NSTIC pilots are implementing the NSTIC principles...

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

Well...

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

Not borrow from what exists today.

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

Also, I would say that internationally there are lots of countries that have identity ecosystems that are way more mature than ours and are already doing this which is part of what spurred the administration to do this kind of thing.

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

Well that's true.

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

So there are...NSTIC, NIST routinely meets with a number of countries globally that have these infrastructures already in place and there is a list of who they are but I'm just saying generally that, you know, we're behind which is why we're doing this.

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

Are there specific...

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

This is Jeff what is NSTIC?

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

The National Secure...

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

The National Strategy for...

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

Strategy, yeah, Trusted Identities in Cyberspace.

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

Identities in Cyberspace and if I could...

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

The National Identity...

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

The National Strategy for Trusted Identities in Cyberspace.

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

Okay, thank you.

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

I can...yeah and it is NSTIC.org.

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

Thanks.

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

This is Jason...

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

And there is a health committee that, you know, anyone could be involved with.

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

NSTIC is a White House Initiative initially, it was a White House Initiative and the idea was to provide standard kind of identity credentials and means of identity proofing so that these credentials could be used across multiple purposes. So, you might get a credential for your bank that you could then use in healthcare or you could get a credential from healthcare that you could use in your bank to prove your identity.

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

And ultimately it would be managed by the individual so you could actually set it up through a portal or something like that and use it everywhere. You know we've had a couple of briefings on this and I can certainly talk with anyone who wants to get more information on it. I think we should, you know, just sort of move forward with our...

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

And we should also...

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

Work.

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

For about the last two years, at least, just about everything the Security Working Group has been asked to do by the ONC has included the phrase "consider NSTIC" in your response. So, the healthcare industry is going toward NSTIC very...is pushing NSTIC pretty aggressively.

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

So, this is Jason and I want to lend full support to what Lisa said about how the healthcare industry is different. That said I think there are some things that we can learn from the banking industry and some questions that we ought to be anticipating and answering in regard to this question that was put to us.

A couple of things right off the bat that are very different, if you think about the money that's in a bank and draw an analogy to the data that we have entrusted to us for our patients there is a huge difference in terms of liability. As a hospital I'm not FDIC insured, right the government is not backing me up, if that money goes missing they're backing up the bank giving patient assurance, but we don't have that in our industry, right?

If you're a consumer, and by the way one of the parallels though is that there are two different kinds of...roughly two different types of transactions, there are those involving the customer, which in this case are those that involve the patient directly, but we also...both of our industries also have back office transactions whether it's a clearinghouse thing in a financial situation or the standard transactions in our business those don't evolve and those are really two different kinds of standards, two different kinds of procedures where this whole proofing for interchange and authenticating those transactions should be answered differently.

In the first one, which is I think what the question is really about whether it's NSTIC or something else the point we definitely want to emphasize is we want a federated model.

If people have already established identity proofing by either in person or on line through knowledge-based or whatever it is and it meets our level of trust for our different assurances, for our different use cases then we should absolutely be able to use it and conversely we want to be able to establish proofs and Trustmarks, etcetera, so that people once they've acquired it through us it can be federated for other purposes and I think that's the real...

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

That's exactly right.

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

Change we want here.

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

Identity federation, right.

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

Yes and that...

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

Now if we could get our industry to give us some liability insurance...

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

Yeah.

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

You know I'd love to have a PHIDC.

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

I'd like to pile on your comment there Jason because, you know, most of my work has to do with genomic data and, you know, when you're talking genomic data that's quite different from...and health data in general, but especially genomic data from a credit card because you can get a new credit card and you certainly can't get a new genome. So, the risk to the individual and their families, you know, their blood relatives as well is way, way more than anything that a bank undertakes.

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

So, when we worked with the Department of Health to do their electronic identity management system the one that they use for the marketplace and they're using for many other things going forward, they used a knowledge-based authentication system whereas a result of that process a score was given and then it allowed, in the government's context each system has its own specific business owner but you could apply that directly to a commercial setting where each of us would get to decide for ourselves whether that score was sufficiently high to allow us to trust that the identity was really that person and move forward or whether we had to push back for a higher score.

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

That's what you...I missed the point, that's what you did or...

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

That's exactly where those things are working and I'm suggesting that's a very similar approach that we would want to take here, this should...again, we're not a one-size-fits-all model and the solution...the token itself can be, you know, isn't the point it's not about the strength of the physical thing that gets presented it's about the level of rigor that happened when we bound the identity to that token.

So, if somebody went through a question and answer process at a bank say and we now want to trust that identity for our purposes we need to understand the scoring behind it so that we can make a decision about whether that's sufficient for our use case.

I may say it's okay for you log into your own personal health record to enter information about, you know, how many steps you walked in a day. I might not let it be okay if you want to pull stuff out from an EHR and if it's genomic data, to your point, probably not, if it's a low score, right?

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

Yeah, yeah and that's part of the whole NSTIC model too so that you could tell by a certificate the strength of the identity proofing that went behind it.

Now one of the things that banks typically do and people expect them to do is to check your credit scores, you know, in giving you a loan or whatever and in healthcare I know that there is pushback from people, you know, they don't want any overlap between their healthcare and their financial, they don't...they specifically don't want healthcare to be checking their financial data or vice versa for that. So, there is also that, you know, line that needs to exist between the two as well I think.

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

Right, we weren't suggesting that we were simply suggesting if you used I don't know Fidelity for your on line banking or your stock transactions or whatever and they established an identity that was good enough for you to get in to manipulate and manage your money we could choose to accept that same identity in a federate model for giving you access to your health data.

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

Yeah, I know, I knew that's what you were saying I was adding this to the differences between healthcare and financial.

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

Right, right.

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

So that's another difference is that people don't want...

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

...to same thing, they also don't want us going and evaluating their social media even though I think legally that's considered to be information in a public domain. I think a lot of people have the concern or the perception that it's really private data that they should have control over and we shouldn't be able to go to their Facebook page and use that as a basis for proving that they are who they say they are or not.

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

Yeah, yeah, well they don't want their bank doing that either. They think their social media are private, silly them. So, we've addressed how healthcare is different and what ID proofing and authentication standards, policies and protocols can we borrow and we've also said that we don't want to borrow from what the other industries do today but we want to look at how industries are implementing NIST and borrow from their plans. Is that right? Did we capture that?

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

Yeah, I think that's fair.

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

This is John...

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

I think that's a fair comment, Dixie.

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

Okay.

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

Dixie, I agree, sorry, this is Scott, I agree, I think that captures it. One thing that we do want to facilitate I think is to have an understanding of what other industries do and, you know, if industry "x" calls these type of provisioning processes level A and the healthcare industry calls it level 3 I think it's good to understand that mapping so that when you have an opportunity potentially to accept a process or a credential from another industry you have a comparable means of understanding what that means to the standards that are set within healthcare.

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

Yeah, yeah.

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

Yeah and that's a really good point but just so that you all know NIST is looking at their own document and trying to determine if they need to move away from levels of assurance and go with this concept of componentized trust. So you take, you know, you define the identities by the components of trust that are included in it and not some level but anyway there is a common way to describe it which is in this 800-63-2 or whatever it is, but they're looking at redoing that and we're tracking that as well. So, there is a lot of movement here I think and it's all very positive.

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

You know...

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

You know I think point here that we've all hit on that I think is fair, Dixie, that second question is healthcare that different, it is because healthcare is very personalized and not that banking is not or social media is not and when it comes to your health data, I mean, people get up in arms quickly about that versus if you get your e-mail hacked, okay, that stinks, whatever, you know, your social media gets hacked yeah it's an annoyance, whatever, but someone gets your records from birth I mean that's, you know, hell hath no fury basically. So, it is that different and it needs to be treated with that same level of care.

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

Well, the thing is...and I'm not, as Lisa will tell you, I'm not...I don't have much practice at being the Devil's advocate but I have to tell you if you look at all of the breaches that have occurred there certainly has not been the outrage that I would expect from the people effected. I mean, we just...reporting a breach has just become common, you know, workflow anymore, report this breach.

The number of people that have been affected by breaches is tremendous and I certainly don't see any pushback. I also don't see people shrinking from, you know, using Apps, using mobile Apps and Fitbits, and all of these devices that they know darn well the organizations that have given them those Apps and those devices are selling their health data. I don't see much pushback there.

So, I think in some ways people are schizophrenic about this or head in the sand, or something because people...if you ask them they certainly claim that their health information is really important to them but their actions don't say that at all.

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

Fair enough, I just wonder if the general public actually understands. I mean, I think they're beginning to understand but we're just now being made aware of what's been going on in the industry for decades.

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

Yeah.

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

And, I mean our tools are now sophisticated to catch these things. I mean, it's always been, hey, you know, 1000 records falls out of a box, in a cardboard box off the back of a truck, you know, oh, it winds up on the side of a highway that's been there forever now it's just electronic.

So, to the degree of it I agree with you but what I was talking about though in terms of that difference it's personalized, you know, to get a mortgage on your house you're filling out, you know, 100 different forms.

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

Yes.

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

You know social media is whatever, you know, you can create a new e-mail account in a heartbeat on G-Mail. I mean, healthcare is more personalized and that's what I was trying to say is that...to whatever the degree is I don't want it to be lost in touch that we need to not be creepy with the way we handle this that's all, that's all I'm saying.

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

Yeah, I totally agree with you. I just get frustrated that we don't see much, you know, that having to constantly deal with the comment that, oh, people don't care that much about their healthcare information or else they would...you know, I get that all the time and I'm constantly dealing with it and I have to say that, you know, that's a good point, you know, people...

M

Yeah the other...the other thing to consider is the whole issue of patient choice. I mean, I think that we want to be able to provide these robust identity proofing solutions and yet we don't want to necessarily always require them...

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

Yes.

M

Because, I mean, as a provider who interacts with, you know, 90% of my patients on line on a regular basis, you know, patients only have so much tolerance for, you know, the login, the sign up, the management of all this. So, I mean, it's tricky, we don't want to make this so onerous that it prevents people from utilizing it, but we also want to be able to provide the depth of security tools that are available for those who do.

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

That's the beauty of this is that it would if, you know, one more sign up process and it would eliminate the 35, you know, accounts you have for various merchants on line you would use the same identity and assert it in different levels of assurance in all of your transactions including healthcare.

So, that is part of the consideration and you also will have likely, you know, a good percentage of the patients will already have this identity set up through other means whether it's, you know, a bank that helps them set it up or if they learn about the function in the portal and they go and set it up themselves they can start using it and they can start...they'll start presenting it at healthcare organizations, you know, it's part of what they do every day. They may have a chip on their phone or a smart card or something that would allow them to present it at the time of identification, at time of payment or things like that everywhere.

So, it's designed to...it will be rolled out in the eCommerce space and then it is something that could be leveraged in healthcare without requiring additional steps if it could meet our goals. Does that make sense?

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

But I do think that that's an example of why...you know you say, well my patients...I don't want my patients to have to go too much trouble but most of patient portals don't meet the...are not as...don't have the level of security that banking portals do and I think if you implemented there at your office, if you implemented exactly the same security authentication that is commonly implemented for banks the patients wouldn't think of saying, oh, that's what they would expect because that's what they get for their on line banking, but the healthcare industry pushes back on that. They go, oh, I don't want my patient to have to go through two steps to get into the portal, well they do that all the time when they go to the banks.

So, I think that we...when we say all our information is much more sensitive, which it is, than banks and we need stronger than what the bank does on the one hand and the other hand our providers refuse to implement the portal security that's equivalent to banking, I think it...we kind of make people crazy. I think we need to be consistent with our message.

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

I think this is going to take care of itself because I really think that anyone who does eCommerce, you know, or orders stuff on line is going to end up having one of these identities in the next couple of years and start presenting them in healthcare organizations. So, it's going to be driven by our own patients and consumers that's why...

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

That's a...

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

We need to be paying attention to it.

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

We should capture that as our summary. Okay, do we have time to start the next one, G? Let's go to the next one. Okay, oops, there, can we go to the next slide? Oops, last one, one before that. And this is Section G we were asked two, three questions about consent.

What standards should be put forward in the 2016 standards advisory for basic choice? How much work should ONC be doing on other standards while clarifying permitted uses? If standards development needs to be done what should we be working on, data segmentation for clinical decision support versus data segmentation for privacy versus something else?

Now data...for those of you who may not know, DS4P, data segmentation for privacy is a profile that was developed by the ONC last year. The DS4CDS, as far as I know, doesn't exist I think it's just an example, right?

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

That's correct.

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

Okay, okay. So, let's go to the next where it's a little easier, next slide I think is a little bit easier to read. Okay, what standards should we put forward in the 2016 standards advisory for basic choice?

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

And can someone define the term basic choice, what exactly are we talking about here?

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

They mean consent, but the trend these days, you know, the...when you mention the word "consent" people usually think of a piece of paper that you sign and there you're gone, you're off and running, the healthcare organization files it away and, you know, it's done. And so there is a trend to move away from the word "consent" toward choice or permissions, or something that means more a richer set of choices than just yes/no sign the consent form.

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

Yeah and this is Jeremy...

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

Well...

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

To add to that a little bit, so in the roadmap we outlined this kind of three tier structure around, you know, consent for data sharing and the most basic level is what we're calling the background rules so those are the rules that if a patient does not express any consent what rules govern the data exchange because HIPAA does allow for example, you know, exchanging data for treatment, payment, healthcare operations.

Basic choice is your next level up which is simply a binary decision by the patient, do I want to share or do I not want to share and then granular choice is the next level where a patient says, you know, I want to share, you know, my family health history but not my behavioral health notes for example. So, that's all outlined in the roadmap.

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

Yeah...

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

So, are we basically saying that the proposal is...that we want to implement a standard of basic choice for 2016 presuming that it subsequently will look at more granular choice?

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

That is correct, yes...

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

And so Jeremy, my question, this is Lisa, my question on when you get to granular choice what is the policy lever for that because we don't really...I mean, we keep saying we're going to do it but we don't have a requirement to do it. So, I'm trying to figure out do we need to answer that question too?

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

No we don't, so Section G is being commented on by both the Privacy and Security Workgroup underneath the Policy Committee as well as our Workgroup and so our Workgroup is focusing on the standards questions around consent and then the Privacy and Security Workgroup is focusing on the policy questions around consent so that specific question is being discussed but in that other Workgroup.

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

So, then we can assume that, you know, there is going to be some policy lever for granular consent and try to figure out if there are standards for it?

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

Correct, yes.

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

Well, I...

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

So, Jeremy, this is Aaron and I appreciate the...this is a tough thing to get through and I appreciate that, I just want to give you some feedback in general though, I also sit as the Vice Chair of the Public Policy Committee for HIMSS and I can tell you there is a lot of confusion around this topic so whatever you can do to help clarify for folks, especially in HIMSS and CHIME, and others say what these choices are and how they don't override state or federal privacy law that's already established and this is more of an augmentation of that, more granularity around it, I think will be very beneficial to getting adoption in the community. So, just some feedback for you.

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

Yeah, I think that...

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

Yeah.

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

Most of my work is around granular consent but it has to do with granular consent for research.

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

Right.

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

And I totally agree and understand all of these arguments that if you are a healthcare organization and you have liability issues around the decisions that you make based on the information you have available I do understand why that pushback is coming.

I think that, and Jeremy maybe I'm talking to you about this, but I think that we...that there is a real need to communicate that there are other reasons why you would want granular consent besides just blocking off from a doctor, you know, like you may want to allow your data to be used, for example in the work that I do, for cancer research but at USC but for no other reason, you know, there are...and that has nothing to do with the delivery of care and it's not going to affect liability but it's going to make it easier to make healthcare data available for research and so I think that we need to get passed this idea that there is a bugaboo, somebody out there trying to keep doctors from getting the information they need to make sound clinical decisions...

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

Right.

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

I think that's really important.

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

I agree, Dixie.

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

So, the question at hand...sorry the question at hand here though is not about those advance choices or more granular choices this is, you know, what standards could we put forward in terms of basic choice and I think I heard the explanation...

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

Well granular choice...

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

Of what basic...

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

Granular choice is on the roadmap, so that's like, you know, the third column or whatever.

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

Okay, so but...

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

I think what they're asking...

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

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
I hope that that's what...

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
Sorry, for this particular question I wanted to propose that we should at least, one standard that we could potentially put forward in answer to this specific question is that, you know, some time ago there was the ESIGN law that came out, we know what a digital signature is and then we have electronic signatures and I think that we should look to the guidance and controls around electronic signatures as being one aspect of basic choice as a standard that should be followed.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
I think the first thing that we should do...and I agree with that. I think the first thing is that we should say that standards to enable consent to be electronically captured, used and exchanged is the basic thing that we should be pushing for instead of these paper, because you get...I've been in many conversations where when you talk about electronic consent they're thinking, oh, I scan in this paper and it became a PDF and I jam it into a CDA and send it across the wire, well, no, you know, ISO has some standards for consent, HL7 is starting to adopt some of those standards. I think we need to push towards standard ways of capturing, you know, using...capturing, processing and exchanging these consent rules.

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

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
Yeah, A+ on that.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society
Scott that's exactly right and that's how we can stay away from the policy question and just contribute where there are technical standards that can be leveraged. That's exactly right, thanks.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Other comments about that?

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center
I mean, I just go back to a standard of education or awareness, or something like that, because I can just see, especially sitting, you know, in the chair I am and the folks I talk to a lot of confusion and I can see the public having a lot of confusion even as basic as this is. So, from a standard level, a standard of education or awareness, or something around it.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Yeah, I totally agree. There is so much misunderstanding and paranoia around this, yes. Well, I have 25 after so why don't we hold the other two questions. Are we supposed to address the other two questions, Jeremy?

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

Yes.

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

Yes, but we do have the time in our next Workgroup meeting reserved for anything that we didn't get to.

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

Okay, so for our next Workgroup we'll capture these comments that we made today and we'll move onto the next two questions and possibly also address some of the specific recommendations that ONC has made if we have time. Okay?

Well, I'd like to thank all of you for your...this has been a wonderful discussion so...and I have all kinds of notes and I pity the ONC team having to capture the salient points, but we'll work with the ONC team and try to convey your key points as best we can in the next version of the straw recommendations. Are there other...Lisa, did you want to say anything?

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

No, Dixie, I would like to echo what you said, I think this is a wonderful group with, you know, a really good perspective and I appreciate everyone's participation this has been great, thanks.

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

Yes, okay, shall we open it up for public comment?

Public Comment

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

Operator can you please open the lines?

Caitlin Chastain – Junior Project Manager – Altarum Institute

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

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

It looks like we have no public comment.

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

Okay and our next meeting is March the 25th, so I hope all of you can make that and thank you very much again. Bye-bye.

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

Bye.

M

Bye, everybody.

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

Bye.

M

Thank you everybody.

M

Bye, thank you.