



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
February 24, 2015**

Presentation

Operator

All lines are bridged with the public.

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

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Standards Committee's Transport & Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the meeting. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. Also as a reminder, if you are not the person speaking, if you could please mute your line it would be appreciated. I'll now take roll. Dixie Baker?

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

I'm here.

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

Hi, Dixie. Lisa Gallagher is on. Aaron Miri? Boban Jose? Brian Freedman?

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

Here.

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

Hi, Brian. Jason Taule?

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

Good afternoon.

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

Hi, Jason. Jeff Brandt? Jeremy...I'm sorry. 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?

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

This is Aaron Miri, I apologize, I'm joining late. This is Aaron.

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

No Lee Jones though, right? Peter Kaufman? Scott Rea?

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

G'day, I'm here.

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

Hi, Scott. Sharon Terry? Steven Lane?

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

Here.

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

Hi, Steven. And from ONC do we have Jeremy Maxwell?

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

Here.

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

Hi, Jeremy. Anyone else from ONC on the line?

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

Hey Michelle, it's Julie.

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

Hi, Julie. With that, I'll turn it back to you Dixie.

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

Yeah, I just want to mention I did get an email from Peter Kaufman who said he may be joining a few minutes late, he has another meeting but he will be dialing in.

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

Thank you.

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

Okay. I want to thank you all for dialing in today, today is the first day that we...is our launch of our review and comment period for the interoperability roadmap that was recently released by the Office of the National Coordinator. Hopefully you've had an opportunity to look it over. Specifically today we're going to talk briefly about the timeline for our comments and what ONC has asked us to comment on and then we're going to launch into the discussion specifically focusing today on section E. And so that's our agenda for today. Lisa, did you want to say anything? Lisa's sick, I should tell everybody, so...but thank you for joining us anyway, Lisa. Well, maybe she isn't.

So, with that, let's just launch into our discussion here. Next slide. Okay, for those of you who have either read the roadmap document or have watched it...or listened to the Standards Committee review of the roadmap, which was given at the Standards Committee meeting 2 weeks ago, you'll see that the whole...the interoperability roadmap really centers around some...10 basic principles that are depicted on this slide.

They want to build upon existing infrastructure and very closely related to that is to consider the current environment and support multiple levels of advancement. What they really...the clarify the difference between those two, because obviously they're very, very similar is that building on the existing HIT infrastructure is really building on the EHR standards and the technology that's in place. The current environment goes beyond technology to include other considerations as well. Protect privacy and security of all aspects of interoperability. Maintain modularity. Empower individuals. Leverage the marketplace. They want scalability and individual access. They recognize that one size does not fit all. They want to simplify and finally focus on value.

The other basic principle, although it's not the same type of principle, but the focus that you'll see throughout the roadmap is a focus on kind of an end state of the learning health system. And for those of you who may not be familiar with that, that basically is a state in which we collect data regarding the treatments and outcomes and we continuously improve the quality of care by feeding those outcomes back into the system so that the system itself becomes kind of organic and is able to learn as time goes on. So, next slide, please.

The lead for this...for our Transport & Security Standards Workgroup is Jeremy Maxwell, who's on the call today and we identified the ONC's subject matter experts are Julie, who's on the phone today, Chris Muir and Lucia Savage, who is the Chief Privacy Officer for ONC. They ask us to address, this workgroup to address a number of questions. One is are the actions that are proposed in the draft roadmap the

right actions to improve interoperability nationwide in the long term, as well as working toward this learning health system? These are the questions that they ask...I think they ask these to everybody in general and then later we get on to the specific ones as to us. The second one was what, if any, gaps need to be addressed? Is the timing of specific actions appropriate? And are the right actors and stakeholders associated with critical actions.

Then the roadmap sections that were assigned specifically to the Transport & Security Workgroup were sections E, F and G; where E addresses the ubiquitous...the need for a ubiquitous secure network infrastructure. F focuses on identity and authentication and G is consistent representation of permission. These sections, I believe begin on page 55 of the roadmap, and hopefully you've already looked them over. Next slide, please.

Section E addresses two...the address them as separate topics, my own opinion is that encryption is part of cybersecurity, but they address it as two different topics; cybersecurity and encryption. And the specific questions are, with respect to cybersecurity, what should the federal government specifically focus on first to move towards a uniform approach to enforcing cybersecurity in healthcare, keeping HIPAA and the Certified Electronic Health Record Technology rules in mind and possible new cybersecurity legislation? Are there frameworks, methodologies, incentive programs, etcetera, that the healthcare industry has not but should consider? And then in the encryption area, are there other gaps, aside from lack of policies and guidance for implementing encryption in technology and standards for encryption?

I was wondering whether Jeremy you and Julie perhaps could clarify more what ONC means when it says in the first question, keeping HIPAA and certified EHR technology rules in mind and possible new cybersecurity legislation? What exactly do they...the meaning of that?

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

Sure. Julie, this is your area of expertise, do you want to field that question?

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

Sure. Hi, Dixie. So in terms of the parenthetical in there, where we say HIPAA and the CEHRT rules, we just wanted to make sure that anything that the workgroup does recommend in...for this question keeps in mind that HIPAA does have some enforce...OCR has the enforcement arm for the HIPAA security rule and the CEHRT rules also have certain limitations as to what ONC specifically can do.

In terms of possible new cybersecurity legislation, I just wanted to make sure that the workgroup did know that the current administration is focusing a lot on proposed legislation around cybersecurity. As you all may know, there was a new Executive Order that was signed two Friday's ago regarding information sharing. And there are other legislative proposals out there that may impact the work of this workgroup as we go through the comment period. In terms of specific legislation, there is not one specific one that I would point out to, but just more of a broader sense that this cybersecurity is a hot topic these days; so we want to make sure that any recommendations either don't negate anything that comes out or is not impacted by anything that comes out while we're doing this. Does that help, Dixie?

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

Yes.

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

Okay.

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

Yes, I do know that the White House had a Cybersecurity Summit last week or the week before, so yes, I suspect we're all aware that there is a lot of emphasis on cybersecurity. Okay. So this workgroup previously has commented on the fact that EHR certification does...of modules of EHR...is limited to modules of EHRs and security is not required to be included in certification. That, I presume, is off the table at this point because our comments haven't...has been heard...have been registered before, right?

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

Yes, Dixie, this is Julie again. So we are expecting the NPRM to be out sometime soon, so I think that's the best forum if this workgroup would like to revisit...

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

Okay.

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

...that topic, so, I'm sure Jeremy has that noted already.

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

Yes.

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

Yeah, I think he mentioned it before, but I wanted to make sure that others knew that as well, so...

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

Yeah, great.

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

...we will have an ample opportunity to address the full certification of EHRs and...at a later time and specific certification requirements as well. Okay, so section F has to do with ID proofing and authentication standards, policies and protocols. And they're asking what ID proofing and authentication standards, policies and protocols can we borrow from other industries? Is healthcare that different from banking, social media or email?

And section G, what standards should be put forward in the 2016 Standards Advisory for basic choice. How much...in other words, individual patient, if you will, or consumer 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 like DS4CDS; in other words, data segmentation for clinical decision support versus data segmentation for privacy versus something else? Now we're not going to address the section F and G this time, we'll be addressing those later, but today's discussion will be focused on E. So next slide, please.

Ah, speaking of which, here's our timeline. Today's meeting, as I mentioned, focuses on section E. Our next meeting March 11 we'll be discussing sections F and G. March 25 we are holding the workgroup time for additional discussions and final review of our comments and any other items that may come up. As it was asked at the last Standards meeting, it was asked whether our comments...the workgroup comments need to be...and the committee comments, need to be restricted to specific questions that are asked of us.

And the response was, they don't need to be restricted, but ONC's priority is to get answers to the specific questions that they ask. So it's imperative that we give well thought-through answers to the specific questions asked first and then if there's time, we can talk about other issues that people may want to comment on or discuss. And then the comments need to be completed and submitted by April 6. Is that the due date for them, Julie? Is April 6...

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

This is Michelle. That's the public comment due date. For the FACAs, though, the due date will be at the April Standards Committee meeting, which is April 22.

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

Oh, good, good. Okay. Okay. Thank you. Okay, next slide, please. I'm making myself a note of that so I remember. Okay, the interoperability roadmap section E; section E is devoted to ubiquitous secure network infrastructure. The learning health system requirement is, ubiquitous secure network infrastructure is enabling an interoperable learning health system requires a stable, secure, widely available network capability that supports vendor neutral protocols and a wide variety of core services. And the specific charges; are first in cybersecurity, second in encryption.

In cybersecurity, what should the federal government specifically focus on first to move towards a uniform approach to enforcing cybersecurity in healthcare, keeping in mind HIPAA and Certified EHR Technology and possible cybersecurity legislation? Are there frameworks, methodologies, incentive programs that the health industry has not, but should, consider? Okay, let me open the floor up for discussion about this first question...first set of questions; the first set of questions regarding cybersecurity. Is Peter on yet? Okay, is there...I'll wait a minute, because I do have his comment. Are there any who would like to...is there anyone who would like to open the discussion regarding cybersecurity?

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

This is John Hummel and I'd like to make a comment. When they rolled together cybersecurity and then they have the discussion around secure network infrastructure that tells me that they're looking for a technological standard that the EHRs would have to be able to be operated on. And so it is that type of

recommendation they're looking for is that specificity or are they looking for just, gee, EHRs should sit behind a DMZ to be secure, something like that?

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

Well sitting behind a DMZ is not network infrastructure. I think what they're talking about is things in front of the DMZ, you know, the network infrastructure that connects...

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

Um hmm.

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

...from the front door of one healthcare organization to another.

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

So, this is Aaron Miri and let me kind of just take a step back. Dixie, I like where you're going with it, sort of a more holistic, universal approach. Let me put this out there that beyond the EHR, beyond that, you've got medical devices; you've got a litany of things that are coming in to a healthcare environment that might not be going into a typical office/corporate environment. So I think for whatever, if there is a standard or there is an enforcement, it has to be across the entire continuum including a standard that even wearables and others can all adopt because unless you get that uniformity and conformity, we're always going to be facing a battle.

And that's a problem is that right now, everybody wants to bring everything into our environment and if you dare say no, you lose the providers and the providers already a dwindling number. But if you agree with it, with whatever we recommend and whatever this comes out, it must be something that's acceptable across the entire spectrum, beyond EHRs.

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

Yes. Yes, in the roadmap, it does...the roadmap does recognize this litany of things, exactly what you're talking about. It does recognize that as a reality so I think that...I totally agree with you that anything that we recommend needs to really approach that sort of network infrastructure, as they talk about, but it is more of an ecosystem of exchange infrastructure that exists that they're really driving toward. Fortunately, the powers that be that wrote HIPAA, in my opinion, did a really good job of anticipating this...these dramatic changes in technology because HIPAA itself is based on risk management, a risk management model that says, no matter what technologies out there, you need to do a risk assessment and implement countermeasures to your risks based upon the risks that exist.

So I think that...I think we need to take the same approach, that risk management kind of a model that regardless of what's out...what's...wearables or Fitbits and mobile devices and the whole ball of wax, anything that we recommend needs to recognize that that's what we're...that's what the infrastructure looks like.

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

Absolutely agree, Dixie. This is a follow up, again this is Aaron. I would encourage us to have open discussions with members of the Office of Civil Rights and others to again give some sort of acknowledgement that if an organization does a risk assessment on say a device that's more of a...I'm going to call it more of a biomedical or clinical technology that cannot be encrypted or whatever standards are out there, and we do an RA and then heaven forbid something actually does happen and

the data is lost, but again the organization has given some sort of acknowledgement that you did your best effort, you followed all the guidelines and we're not going to come after you for civil or monetary damages.

I think right now, especially speaking as a provider as a CIO of a hospital, I could tell you one of the things I fear most is gosh, there's something out there that might have PHI that maybe can't be encrypted for whatever reason and they hide behind, oh, we're FDA certified or we can't encrypt, which is a bunch of baloney, but regardless and there you have it. Now you have a smoking gun. So beyond a technical standard, and I've said this on many, many calls, we must have partnership with the OCR for that recognition, otherwise hospitals are just not going to buy in because they're fearful.

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

Aaron...

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

OCR recognizes that HIPAA is risk-based as well...and who tried to say something, sorry.

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

Yeah, this is Brian Freedman. I mean I guess to go kind of almost the opposite of Aaron, part of the problem is that people aren't doing the risk management or the risk assessment stuff correctly. So I mean, I think that has to be taken into consideration as well. I mean, they do some sort of risk assessment, but it doesn't really...it just doesn't cut the bar and then when they do have a breach, it's clear that there's an issue or even worse, there have been cases where OCR has come in and said, okay, well you didn't do a risk assessment, you have all these deficiencies, go ahead and fix them and then these organizations don't. So, I think that needs to be considered as well.

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

That's a very good point; this is Aaron again, speaking as a CIO for hospital system, you're exactly right and I think we have to...there has to be a level of mutual trust and mutual ownership there and I think credit to the HHS and the OCR and the ONC for putting some much better guidelines...out there, even examples of frameworks to follow and examples of the risk assessment tool and for small and medium businesses; I mean, kudos. But again, more education, more awareness.

So I know we're taking this on a tangent and I'm sorry Dixie, I'm just very passionate about that. In order to get hospitals to share data and really start buying into these things, beyond a technical standard, it just needs to be a level playing field across the entire continuum. That's all.

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

This is Lee Jones, Dixie and I joined a little bit late so I hope I'm not off base but, it sounds to me like this idea of the secure network infrastructure, the general problem of it if you will, is something that was wrestled with when the whole Direct protocols were being arrived at in that we wanted to have secure transport, we needed everybody to sort of agree what that was going to be and they basically settled on the SSL and all that stuff. And then the issue was how is it that you get people to participate in this whole idea of trying to have the distribution of trust anchors be centralized in some anointed group that could certify that people were doing the right things. And then also had the side benefit of propagating nodes in a network...and proliferating, I should say, nodes in a network so that the network grows and grows in a predictable way.

It seems like all of that stuff, having now been done for Direct, the same mechanisms, if you will; the same organizations, the same idea of we have organizations that now trust each other at some level, they share trust anchors, etcetera, etcetera, could be leveraged for this purpose and you could augment whatever other things beyond the transport issue that you wanted to into these accreditations and so forth. So, I'm not sure if this is sort of a new and novel problem, unless I'm misunderstanding what's being asked here.

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

Well actually...

M

Dixie...

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

...what the roadmap acknowledges what a number of us already know, the Direct model really isn't working because the Direct nodes are not trusting each other and in fact, the roadmap even mentions this with respect to authentication and identity management that there is a need for some kind of mutual trust. So, I don't think a recommendation of replicating Direct is going to be what they're looking for.

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

But when you say that they're not tr...I know that there's...so there's certainly a schism in the way Direct is being implemented where some people get these accreditations and some don't, HISP's I mean. And the ones that don't still have their patchwork of HISP-to-HISP agreements or just handshakes and all that other kind of stuff; I'll give you my certs, you give me yours. And some of that stuff seems like it's just because the need for more far flung Direct kind of Direct style communication is just not needed, right? I only need to communicate with my immediate neighbors and so I can do it by just getting this HIE over here to do something...but when you...or when you say it's not working, are you talking about even among the ones who have gone through this...the cost of getting these accreditations and joined in the trust bundles and all that stuff, they still are not trusting one another?

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

Apparently not; I'm not the expert at this but you can look in the roadmap and it does point out how they don't trust each other's identity proofing, they don't...you know, and so what it says in the roadmap. I'm not...this isn't my opinion, what it says in the roadmap is that what's happening is that they're still doing these HISP to...organization-to-organization agreement and there still isn't this...the concept of this infrastructure where everybody shares information and trusts other people's identity and trust other people's security isn't there. I was trying to look through where that is but, it is in the security section, but I don't think it's a...but yeah, I think it's in the identity, discussion of identity.

M

So...sorry.

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

Sure, so, this is John Hummel, I'll just give you a quick example. We're trying to establish from our hospital here in California to an HIE in Nevada and the HIE is unwilling to share any of their HIPAA preparedness, they're not willing to share their risk assessment; before I start shipping my patient's data

over to the repository, I need to make sure that its secured and that they have proper identification and they do proper authentication. And they simply are refusing to share that information with me. So, it's not a trust issue, it's in fact is that they feel if they give us that information, they're going to be revealing possible...potential breaches should they...to have a HIPAA audit. So, it's a problem, I think it's a little bit more universal in the fact that we've created a culture in healthcare where we're going to get fined if we have a breach and therefore we're very secretive about what problems we have in our security.

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

But that's why you have the neutral third party auditor, I mean accreditor who can accredit you and accredit them and you trust that entity to say, yes, those guys are okay; so they don't have to show everyone all of their wares, they show it to this one who certifies that yes, they're fine.

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

Yeah, but there is no...this is Aaron; there is no Sarbanes-Oxley or whatever standard that they're all having to meet, that's the problem.

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

Yeah.

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

Yeah, that's a problem. And the criteria they use for accrediting different ones are different, depending, yeah.

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

That's exactly right, and your risk appetite, right? Again, all the people with organizations who want it to absorb, your risk appetite dictates that and there are certain vendors, because this market...the healthcare market is very, very shallow in certain areas. I mean, you're darned if you do, you're darned if you don't.

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

So what...

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

So Dixie...sorry. This is Scott and I just wanted to weigh in for a second because I was not actually experiencing, on the ground so to speak, that lack of trust of interoperability of those that were accredited under some scheme for Direct, for instance. Those that have been through the certifications, to my knowledge, are all openly trusting those that have also been through the same certifications with no denial of sharing data at all and we're actually seeing growth in that space.

I do want to point out though that it's still a relatively immature community from the perspective that there is a group that was part of an interoperability group, which is quite large, but all of those have not finished the certifications. There is now a small, quickly growing group of those that have finished certifications and certainly there is 100% trust between that smaller groups. In the other large group, I also did not detect any unwillingness to share data, even though the entities that were in process to be certified hadn't actually completed their process yet. So, I'd been interested to see the comments in the interoperability roadmap because that's not what I've actually seen in the community itself.

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

Well I found the paragraph, it's on page 59, next to the bottom and honestly, this exact point has been brought up numerous times in the Standards Committee as well. So, there is a trust issue going on with Direct and I think that...I think we're right to comment on it. I think Aaron's comment was probably right on target, the lack of uniform accreditation standards across all. But I don't think that we should address our comment at Direct in particular, I think they've asked us about what's needed for a national infrastructure that is mutually trusting. I mean, that's what they're really going toward and I think that we should specify what is needed.

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

Dixie?

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

Um hmm, yeah.

M

Yeah, I think that's...

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

This is Lisa, I've been trying to jump in...

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

I'm sorry.

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

Would this be a good time to bring up the NSTIC Trustmarks again and recommend that perhaps they follow that as a way to establish electronically trust between trust frameworks?

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

Yeah, I think that's a great idea. Let's see, this group has had the briefing on Trustmark so we know...

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

Yeah, we had two of them...other calls...

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

I think this was a good application of that.

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

And also...

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

So I do want, sorry, I want to make a comment about the Trustmarks. So there are different levels to the Trustmarks, those where you're doing self-attestation, if you like, don't necessarily have the capacity to

engender trust and that's just...now we're not just talking about NSTIC here, my personal experience with other trust communities that leverage similar schemas would demonstrate that anywhere where you just do self-attestation you don't engender trust, but it's a good starting point. However, if you had a trustmark for entities that were audited against some scheme that the community accepts, then you do have trust. And so if that's where we want to end up, that would be great.

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

Right. Scott, I think that's exactly right and as I said on a couple of past meetings relating to this, there's a framework for this and it would be up to the healthcare community to find what trustmarks and what process work for us, but also I think that NSTIC is charged with looking at this across the Internet, across the e-Commerce spectrum and so we need to pay attention to that in healthcare.

I mean, I think that that would be a good recommendation because it didn't appear in the roadmap, although we gave them input on this, at least HIMSS, previously. So, I just thought maybe it would be worth mentioning again. I think you're right though Scott, there's a lot to be defined about the process, but...

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

Right and this is Aaron, I want to jump in with that, too. And I like what we're talking about here because again, we're defining the rules of the game and let's do the sports analogy, if you're going to play football, you know the rules of the field, you know the rules of the game, how many minutes are in each quarter; I mean again, and that's what we're defining. We're not defining what color the football is or all of that, we're just saying what the overarching rules.

So whether we say follow NIST, follow whatever; again, we do need to be ubiquitous in this because remember, these decision points will drive various vendors to having to make a lot of modifications in their system to conform, to allow for the community to get in that, and that might stifle innovation.

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

So are you recommending...Lisa, are you thinking like you would be...I mean, trustmarks are use case specific so there would be like a trustmark for Direct and trustmark for HIE-to-HIE, I mean, multiple trustmarks.

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

There's...well, the way NSTIC is looking at it now, there are different trustmark types defined, so one for privacy, one for security, one for half a dozen other things. And then...well, if you look back at the briefing that we got, you can select different types of trustmarks to package together to communicate...

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

Right, that's what I was thinking about, that packaging.

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

Right.

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

Yeah.

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

And so...and again, what concerns me here is that time is going by and we're not participating, we as the healthcare sector, in even looking at this and evaluating it and that it didn't show up in the roadmap as a possible 6-year option, which I think we gave them input on. So there are people out there trying to solve this problem and we seem to not know that it's going on. And so I just...for...I suggest that we consider repeating that recommendation and doing it in our direct comments to the roadmap.

I would also say that another comment, with regard to cybersecurity, is just some infrastructure for threat and vulnerability information sharing. Because I've been trying in the healthcare sector to figure out exactly what to tell someone, a CIO to do if they wanted to share threats or to access threat and vulnerability information and there's really not one answer. So, I think we have an infrastructure challenge there as well.

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

But we have...there's another...that's another thing that the roadmap mentioned, ISAC, I think in this section, right? Julie...

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

Yeah, I mean I put it in the HIMSS comments, but I don't really see a whole lot of movement. I don't...so I think just a re-emphasizing.

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

Well Julie, would you like to say something? I mean I know that that was...oh, I know, it's in the...it's on page 57. And I'd like to point out page 57 has explicit recommendations that they've made and one of them has to do with ISAC, Information Sharing and Analysis Center that HHS will continue to support it. Another one that addresses several comments we've made today is that ONC will work with OCR to release and updated security risk assessment tool and hold appropriate educational and outreach programs. So I think that recommendation, which is already in the roadmap, captures a lot of...a number of comments that have been raised today.

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

Well I would say two things about that; one, with regard to the Information Sharing...the ISAC, I've been involved in the attempt to create a healthcare ISAC since...for 7 years or so and it's just not getting any traction so HHS, there needs to be a real implementation that everyone can buy into and participate in and HHS needs to participate, I think more strongly.

And with regard to risk assessment, we're talking about cybersecurity here and not merely HIPAA compliance and I find with organizations that we're working with that the mentality seems to be just HIPAA compliance. So do a periodic risk assessment, etcetera and then not really an awareness that cybersecurity is an ongoing, daily activity; protecting your infrastructure against evolving set of threats. So, we need to help make that leap and anything we can say in that regard would be helpful.

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

Yeah, I totally agree with you that today the healthcare industry is more compliance driven than they are looking at security as a real business enabler. I agree, I think that we should make that, yeah, make that recommendation.

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

So Dixie, this is Scott and I do want to make just a quick comment here to clarify what it is that we're trying to get to at the end of the discussion. Because looking at the slide that we have up there, we've got a discussion about cybersecurity and we've got a discussion about encryption, which would seem to be a particular technology that could also apply to cybersecurity.

Generally speaking in a cybersecurity theoretical or research perspective, there are typically three services that you seek to utilize to create security in a cyber-world and they go under the acronym of CIA, and no, that's not the government agency, it's for confidentiality, for integrity and access control. And we were talking earlier about NSTIC, which focuses on identity credentials and interoperable identity credentials, which falls under the "A," the access control and make sure that the right entity has access to their own data or data that's being allowed to them. So that would be one aspect of the CIA that we talk about.

Confidentiality, you know, you typically in today's world are talking about encryption as a method of enabling confidentiality to exist but of course, you also have to control who has access to that confidential data or who can decrypt it or who can encrypt it, etcetera. And then the integrity services are about ensuring that data doesn't change or that a document doesn't change, etcetera, etcetera. And typically if we at the end of the day are trying to make a recommendation about cybersecurity, I would probably be more in favor of recommending that any approach to an all-around cybersecurity recommendation would have to include something that addressed all of those three services and that all of those need to be considered when somebody has tried to mitigate risks that they identify via their risk assessment.

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

Right, the roadmap talks about all three. And what we're trying to do is focus on the cybersecurity topic first and then the encryption topic and specifically, let's go back to...Scott has a really good point here that the specific questions they've asked, let's address the first question they've asked right head-on. What should the federal government specifically focus on first to move toward a uniform approach to enforcing cybersecurity in healthcare? So we've talked about trustmarks, we've talked about the consistent certification; so I think that those are two specific things that have been brought up, right?

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

Ye...

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

Right, so...a framework, right; what framework we've got to decide upon and consistency across the entire landscape, you're exactly right, Dixie.

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

Okay. So are there other things we need to bring up?

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

You know, I see incentive programs on here, and this is just my perspective, again, this is Aaron and please feel free to debate this, while I think incentive programs are helpful like for things like EMR adoption and other stuff, I feel that best practice to do some of the basic blocking and tackling in today's very electronic, connected world. I don't know if that's incentive...we should incentivize people to do the right thing.

I mean, it seems to me that there should just be a standard enforced and there should be more of a stick approach than a carrot approach that if a respective technology, where a wearable...wearable, a brand new wearable system does not want to use, I don't know, HTTPS versus HTTP or some sort of secure transaction, that they should be...I mean, there should be some sort of penalty against folks that refuse to comply from the onset. Versus reward people for what I see as the basics of technology nowadays.

M

But at the end of the day, are carrots and sticks really any different; it's just a matter of how you refer to it, I mean...

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

I agree, but one will be seen as a cost to the general user, the general community versus the other will be seen as this is the right thing to do, kind of like Sarbanes-Oxley or things like that. I mean, what I worry about is a PCI kind of standard that suddenly you see the banks, like Chase and others, they were PCI certified, sure, but they still got breached, because there really wasn't any enforcement of that.

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

Well and we see from our breach notification, which the last I looked it was like over 31 million people affected and over 1200 different organizations. I mean you would think that that would be a negative...would be sufficient punishment to discourage breaches, but they sure...it sure doesn't appear to me that it sufficiently discourages.

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

Well no, and then...

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

Dixie...

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

...no uniform, there is no uniform standard across the spectrum. Look at what happened to Anthem, they did a phenomenal job of their response, phenomenal job; they still got...stuff still happened to them. But when you look at it, they weren't under the same type of auspices that say a hospital would be if they had a breach that size. So I mean, it's very different; and again, back to the uniformity of the landscape.

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

Huh. Somebody else was trying to say something.

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

This is Lisa. First of all, Anthem is a health plan, so they're covered by HIPAA and so I'm not sure what you meant. But my concern is that there's...it's not that people don't want to do anything, they just don't have the level of sophistication in-house sometimes to do active...fighting the cybersecurity battle every day. And so the ability to get every organization in the health sector there is the really vexing problem.

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

(Indiscernible)

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

Well I don't think they're trying to...I'd like to go back to your earlier comment, Lisa. I don't think they're trying to get to cybersecurity, I think they're trying to get to HIPAA compliance.

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

Right.

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

And HIPAA compliance doesn't at all address things like penetration activities or keeping up with the...

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

Right.

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

...updating your platforms with the latest upgra...security, what do they call it, security...

W

Critical...

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

Right. Patches or whatever. But they don't see, they don't...a lot of them don't have that sophisticated ability in-house and don't really even know what to do. It's not just the small providers, it goes further than that. So, I mean...

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

Lisa, this is John Hummel.

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

Go ahead John.

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

So what I was going to say is that one of the problems that occurs is that I think in healthcare we know that we're supposed to run a risk assessment that should include a vulnerability assessment and a penetration test, but that's not required. And so when you go out to your CFO and say, I need \$80,000 to run a PEN test, the CFO looks at you and says, it's kind of like insurance, I don't want to pay for it if I don't need it. So you have to go through a justification of why you want to spend that money on data security versus a thought for HIPAA. So I think if we can get some type of compliance driven through like the trustmarks and some type of a commitment for a standard for security at a minimum level, I think we'd make dramatic improvement in healthcare security.

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

So maybe that's a comment to this first, you know, the first thing they recommend is, ONC will work with OCR to release an updated security risk assessment tool and appropriate education and outreach programs; so maybe those outreach should include the kind of expertise that tells them or helps them do these risk assessment, do these penetration tests. Maybe we could make a comment specifically targeted toward that recommendation.

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

I think that would help...

M

Well this is...

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

if you take a look at the NIST recommendations. They give you 15 tools that you're supposed to use for vulnerability or penetration test, but these are pretty...to a standard IT person in healthcare, knowing how to run Metasploit or Nmap and some of these other tools is a sophistication that we just essentially don't have, unless you go out there and specifically spend the time and energy and money to get the training for that for your IT security people.

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

So that's basically what Lisa said, so what could we recommend to fix that?

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

No, I think that we're focused too far down at the 10 foot level and we need to go back to what we were saying earlier about having a framework. If you want to engender trust that allows open exchange, you need to have a framework that you work within and generally speaking for a trust framework, that means you're going to have three elements again on it, and I don't know why the number three keeps coming up, but it does.

You've got to have technology that your framework is based on, but technology alone is not going to solve it. You've also got to have policies and processes around how that technology is configured, implemented and managed over time. And then the third aspect that you also have to have, the set of legalities and relationships defining what the relationships between the entities that participate in the framework are and then who takes responsibility when "X" occurs and what the process is for resolving concerns between to subscribers to the framework.

That's a general framework for the trust frameworks and we have to look at some recommendation if we're going to talk about allowing free flow of information. Whatever frameworks we recommend should have all of those three elements and we don't want to get as prescriptive as talking about a specific technology, but perhaps talk in a general sense that a framework should have these components, however you want to do that.

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

Hmm. Well they do talk about...there's a different section in the roadmap that talks about governance, which the last thing that you mentioned, and interestingly, our workgroup hasn't been asked to talk about governance, but it sounds like maybe we...I mean clearly governance does need to address security and trust, so maybe we could make a recommendation that governance include these kind of hmm...

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

Yeah, I'm 100% behind you on that, Dixie. That's exactly...I mean, if we could learn one thing from perhaps the mistakes or whatever failures came out of the impetus to try and get Direct out there, etcetera, it was that governance was the one thing that got punted on. And at the end of the day, it's the governance aspect that comes back to bite.

And you cannot have a trust framework on just technology and policy alone; you've got to have a governance aspect. You've got to know what your role in the system is; you've got to know if "X" happens, who's going to take responsibility for that. Unless you have that and then have some certification against that which is where your trustmarks come in, you don't actually create a trust infrastructure, you create portions of it and then you're opening up holes that people can drive right through.

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

Yeah, I totally agree. Yup. Okay, is Peter on the line yet?

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

Final, yes.

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

Oh, so I haven't put forth your comment, so would you like to put your comment forward?

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

Sure, are they in the slides or should I pull up my own, because I didn't actually have...

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

They aren't, I didn't forward it until today.

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

Okay. Hang on, let me find it; give me a second here.

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

Just talking about the cybersecurity piece.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Easier said than done here.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
Yeah, and I've got...oh here...

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

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
Here it is, if you want me to read it.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
I've got it.

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

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Okay, where...did other people discuss their comments or was I the only one who actually sent anything in?

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
I think we got comments from a couple of people, but we haven't consolidated them. Uh huh.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Okay, well I'll read what I wrote here and you're welcome to...it up if you want to. Although there...for number one, cybersecurity, although there are no levers for non-governmental operations, this is an issue and will hinder successful security and interoperability across practices and healthcare systems. For example, there are many psychiatrists who refuse to bill electronically and now ePrescribe so they won't be governed under HIPAA. This is a disservice to both patients and to the healthcare system and any programs will need to be ubiquitous to be ultimately successful. Sure, this is a policy issue but should be mentioned. See, I'm learning.

In terms of standards, the system should systematically move towards encryption in motion. I'm not as concerned about encryption at rest due to recommendations below: enhanced protection against inappropriate access with NIST level of...LOA3 identity proofing and two factor authentication, which will also require federated sharing of identities, NSTIC NIDESG so each user would only need to IDP once and to carry a single two-factor authentication, I didn't put in token. I mentioned move towards, because this will require time for both standard completion, infrastructure construction and user acceptance.

Basically what I'm saying there is that for this to work well, it's going to need to be ubiquitous. If there's interoperability in the system and somebody can break into one weak area of the system and then come across to other more strongly protected areas, the cybersecurity in the stronger areas makes no difference. So although it's a policy issue, I think we need to push the policy side to move towards requiring a higher level or assurance, a level of assurance 3 at least, for identity proofing and two-factor authentication, which is made much less complicated by the things that are coming out of the identity system ecosys...identity ecosystem steering group, or the NSTIC outshoot, to allow some of these things

to be shared and federated. So people would need to go through one identity proofing and have one token instead of multiple ones.

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

Well we will be talking about authentication identity proofing at a different meeting...

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

Um hmm.

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

...and LOA and two-factor and all that. So this conversation we're really focusing on the healthcare network infrastructure of secur...of...and...

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

Well, but it brings up an issue where of course these things can't be separated, but the issue is that the federal government doesn't feel that it has the right and authority to standardize and require these things on a statewide basis, and the state basis if the states have their own rules. But the bureaucrats at the states, I feel need to justify their own existence by making the rules from other states just a little different so that their state shows that they've been doing something.

And so every state has their own specifications and requirements and standards and there are 70 different immunization systems out there now. And so an EMR, which has to be able to connect with them, has to be able to do 70 interfaces and there are 51 different e-Prescribing interfaces and the PDMPs, only 16 states are using clearinghouses and the others are all individualized and they're not connected.

There needs to be some more than guidance from the federal government here if they want this to work because they have to make it...they have to simplify this and make it standardized across the country, not state-by-state basis. It's easy for one doctor's office to do something with the state, but if they're using an EMR program or practice management program that is active across 50 states, that EMR or practice management is spending all of their time writing interfaces instead of making things like usability at the top of their list.

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

Peter, this is Steven Lane and I agree with everything you said but I guess I want to cycle us back to the question at hand, how do those needs reflect in what we need with regard to the network infrastructure? I mean, what should we be suggesting as a workgroup in order to move us past all of these statewide differences or the specialties that are choosing not to participate.

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

Well there we get into the issue of having a single national standard. I don't think that we're going to be able to have a single national network infrastructure, a single infrastructure that's going to cover the country unless the government decides to do it themselves. So if it's going to be a federated system, it needs to be done better than Direct, where any system can connect with any other system for free just by doing the interface and having the interfaces be standardized. That's an issue.

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

Yeah, we did discuss Direct. We need to move on to the encryption questions so let me summarize. I've captured four primary points that we've talked about today with respect to cybersecurity topic. The need for a consistent framework, the need for consistent accreditation and a consistent framework for evaluating security; consistent accreditation. A third was acknowl...to, well, this was actually the first one that was brought up, to acknowledge the heterogeneity of the infrastructure itself so that any solution would be equally applicable, regardless of what devices were on there. And the fourth was the governance, that that's essential to security and trust throughout the infrastructure. Are there any big...other big, bold, topics that we missed?

With respect to...okay, so let's move on to our discussion about encryption. They ask us one question; are there other gaps, aside for lack of policies and guidance for implementing encryption, in technologies and standards for encryption? Now when I read through this, I thought it was really strange that they have encryption as a separate thing from cybersecurity because it's so essential for cybersecurity. Did anybody else think that that's odd?

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

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

This is Brian...

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

Yeah, me too.

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

...well I thought it was odd. I think they're trying to send a message because people aren't doing it. I mean, I've seen countless organizations that aren't using...they use transport encryption but they're not using any kind of data at rest encryption on their workstations, laptops, all portable devices; all sorts...and then there are all these breaches and if you look at the breaches, how many more stolen laptops do we need to have that aren't encrypted?

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

But they aren't doing a lot of things, you know, that's not the only thing they're not doing. They're not doing a lot of things and I thought it was odd that they didn't address key management, which is so core to effective encryption; if you can't...if you don't appropriately manage the keys.

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

Well there's also the level of the encryption and how strong the encryption is.

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

Um hmm.

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

I've got...when I take a look at all my vendors, I've got some vendors who are using a really weak set of encryption for transmission because it satisfies the Meaningful Use criteria for certification. But if you go

take a look at what NIST recommends you use like an AES or some type of a private key encryption, then you get a stronger level of encryption and you have better protection; but that's not required.

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

Well, AES is, at least for EHR certification, it either has to be AES or triple DES, that's the...those are the standards. So, are there comments relating to encryption, besides what I just brought up?

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

This is Peter; as I had mentioned in my earlier comment, I'm not sure that data at rest needs to be encrypted if the system is appropriately protected. That doesn't stand for laptops and mobile devices, but data in a data center. It does slow things down to have the data encrypted at rest and there are some systems that are hesitant to do that. Certainly it needs to be encrypted in transport and I think as processors get faster, encryption at rest will be less of a problem.

But as I said earlier, the big problem's the human factor, not the standards; that somebody let somebody...they leave their unencrypted tape out or they let somebody have their password or something like that. And if we had two-factor authentication required, that would be much less of a problem.

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

Yeah, I thought that in general and that was another...I didn't have too many comments but the other comment I had was that they didn't tie encryption into risk assessment. They talked about risk assessment as part of cybersecurity, but then they start throwing all these encryption generalities out there and encryption should be tied as much to risk assessment as any other security mechanism, in my opinion. I think they just sort of...let's talk about encryption.

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

So Dixie, I think you hit the nail on the head when you said, the obvious one that was missing there was the key management. So, I think we should add, well if you're going to deal with encryption, you've got to have some type of key lifecycle management and you've also got to have some policies around key recovery and who has access to that and how that's performed as well. And if you have something that's encrypted, that key management should also include some aspect of escrowing keys so if something goes wrong with a bit of hardware that you're using to store your existing key, you've got a backup sitting somewhere that you can recover from so you don't actually lose the data, etcetera. So all that plays into key lifecycle management and recovery.

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

Yeah, okay. Yeah, very well-articulated; I think I captured that whole thing. Good, good. Are there other...let's see, where were the...I keep losing where I am here. Are there other gaps in term...aside from lack of policies and guidance, which is a pretty big gap, for implementing encryption in technology and standards for encryption?

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

I think this is a...this is Brian Freedman again; I think that it needs to be mandated at some level that you're going to do some kind of encryption because right now, the way it works is, it's an addressable kind of thing as a part of HIPAA.

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

Um hmm.

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

And somebody made...I think Aaron made a comment earlier or somebody made a comment earlier about you take these things to your CFO, you take these things to wherever and they're like, well, it's not required by law so I'm not going to do it, we're not going to spend the money to do it. So it doesn't happy.

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

Yeah, that's probably...I think Brian, you've that...speaking of hitting the nail on the head, I think that's probably exactly why they separated...they didn't tie it to risk management but rather addressed it separately and said, do this. You need to encrypt your data, because, yeah, yeah and not allow so much leeway. That's a really good comment. Yeah.

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

Dixie, this is John Hummel. In the original HITSP committees that we started, we've attended, 2008-2011, all three states of data were supposed to be encrypted and that got changed later on to the addressable, but it was originally part of the requirements that anywhere your data sits for your EMR, it had to be encrypted.

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

What's this, I heard about in...at rest and in motion, what's the third state?

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

Data destroyed.

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

Oh, well...

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

You have to be sure that your hard drives are completely and utterly destroyed.

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

Yeah, but that's still at rest.

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

At rest, yeah.

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

Yeah, yeah and if it's destroyed, that's even better than encryption.

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

Yeah, at that point it's...

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

Yeah, so if it's at rest, it's in use or it's in transport; those are the three.

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

Yeah, I see.

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

So the last one is rest in peace.

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

Yeah, at rest in peace, good, yeah. Now I thought also, I've always been taught that there are really three things, there's the strength...that determine how good...how effective your encryption is going to be; it's the key management, the strength of the algorithm and the third is how it's integrated into the system. In other words, if it's integrated at the application level, for example, in software at the application level, it's not nearly as strong as if it's in hardware. So, and I don't think they address that third one either, you know, how it's...but I don't know how they could do that.

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

So there is another aspect that surrounds it, it's the management aspect. Sorry, this is Scott, again. And that is how you actually provision keys and I know that's part of key management, but there's also a governance aspect in terms of who has access to those keys and how you do that provisioning as well.

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

Yeah, governance relating...yeah, that's a good point. Yeah.

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

So there's no point encrypting your everything at rest, in transit and on death if you hand out that key to the janitor as they walk in the door.

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

Yeah. And that's...yeah, that is...its part of key lifecycle management, but at the same time, it's also governance goes beyond key management; I think that's...good point, good point. Are there other points we want to make aro...go back if you'll, those of you who have access to the document, if you go to page 57, there's a table and perhaps we could just go down this list of their recommendations and make sure that we've considered all of them. Let me start, I'll just read them so that you don't have to be...

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

And Dixie.

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

Uh huh.

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

That table is repeated in the slides.

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

Oh it is, okay, could you bring that up.

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

Yeah, if you advance the slides maybe 2 or 3 slides.

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

Okay.

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

...that table in there.

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

Yeah, that would be great if you would advance the slide to that. This is our form that we use, keep going.

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

Right here.

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

There. Good, excellent, thank you. Okay here are the, it's hard to read on my laptop. But the first one is, ONC will work with OCR to release an updated standard...or Security Risk Assessment tool and hold appropriate educational and outreach programs. Is there anything else we want to say about that specifically? Okay, the second one is, ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response on priority issues related to cybersecurity for critical public health infrastructure. And really our, yeah; we've been talking not about public health but really about healthcare.

The third one is HHS will continue to support, promote and enhance the establishment of a single health and public health cybersecurity Information Sharing and Analysis Center, ISAC, for bidirectional information sharing about cyber threats and vulnerabilities between public health and industry...healthcare industry and the federal government. Now ISAC, for those of you who aren't familiar with them, they came about maybe 15 years ago, some time ago and the fed...the financial industry has had a very active ISAC for a number of years, probably a decade and as Lisa pointed out, there has been a healthcare ISAC for almost as long a time but it hasn't been...so I'm not sure about the establishment of a single ISAC. What does that mean, Julie, you are the one...you're involved in the ISAC. What does it mean establish since they're already...?

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

Hi, so yes. So right now what we're trying to say with that critical action is that we, HHS, are aware that there are a lot of organizations that have ISAC capabilities and they are formally known as ISAOs, Information Sharing and Analysis Organizations, which are not sector specific. So as you say that there is a health and public health ISAC that exists right now called NH-ISAC.

But we do know that they are ramping up in terms of their capabilities, but they're not as mature. And what we are trying to do within HHS is trying to see what else can we do to enhance and make sure that

the health and public health sector does have a more robust infrastructure. As Lisa earlier mentioned, there have been attempts to do this within the HPH sector, but it has been a challenge and we are recognizing that and we're trying to actually work within HHS, as we speak, to see how we can "solve it." Because...they have their own activities within HHS as they share threat information to stakeholders, but it doesn't reach the entire sector. So that's a little bit of context with number 3 and what we mean by enhancing an information sharing capability within our sector. I hope that helps. So I just wanted to actually say that for the workgroup, I guess documentation and recommendations. I do believe that that is a strong one to include if the workgroup decides to do that.

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

Um hmm. I think part of the...part of it is an educational issue.

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

Right.

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

I don't think...I think that probably most healthcare organizations have never heard of an ISAC.

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

Yeah.

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

And if they have, they may not know that these are anonymous, that you can report your intrusions and your...you can report things anonymously to the ISAC.

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

Right. Sorry.

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

This is Lisa. One other challenge, Julie, and this is for you, is that there are other sources of threat data that aren't integrated into the ISAC.

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

That's right.

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

So we know that the FBI, for example, notifies entities directly if they see a threat against them. They put out bulletins in regional areas, so they're not integrated and so the question is; what is the one

source of truth for threat data? Can't have healthcare organizations having to sign up and log in to multiple sites and try to go through all that information and figure it out. We need to have a place where they can go and I don't think it starts with information sharing, I think it's...because they don't really have any information to share, most of them...

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

Right.

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

...it has to do with getting in the habit of monitoring for threat information and incorporating that into their daily activities.

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

Exactly.

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

Good point.

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

Yeah.

M

Agree.

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

Okay. The next...

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

...some comments on that one.

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

Pardon?

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

I can write up some comments on that one; it's Lisa.

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

Okay, good. I've gotten some notes here. Good, that would be great. Lisa will write up. That would be great, thank you. Next one is, ONC will work with NIST and OCR to finalize and publish the NIST Critical

Infrastructure Cybersecurity Framework and Health Insurance Portability and Accountability Act, Security Rule Crosswalk. What's that?

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

Okay, hi Dixie, this is Julie. So what we are trying to do with that is we recognize that the cybersecurity framework is something that is useful and valuable to use for the health and public health sector, so we're trying to work with OCR and NIST to hopefully do some sort of crosswalk. Because right now, the framework it maps to like ISO standards and the NIST 800-53 publication, right? So we're trying to see if that would work with a crosswalk with the Security Rule. And if not a specific crosswalk, some sort of guidance as to how healthcare stakeholders can use the cybersecurity framework.

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

So if there are gaps...

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

Um hmm.

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

...things that don't map to HIPAA, which I suspect there are...

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

Um hmm.

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

...will that result in recommendations...

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

Right, right, so those are included in the discussion to make sure that if there are gaps that OCR would either provide guidance or kind of a, it is a gap, but it doesn't mean that you shouldn't adopt it or you shouldn't address it. So it's a lot of intricacies but that is something that is also being worked on.

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

Okay. So are there any comments about that? Okay, and then the last one under cybersecurity is HHS will work with the industry to develop and propose a uniform approach to enforcing cybersecurity in healthcare in concert with enforcement of HIPAA rules. I think that that's where our comment about governance goes.

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

Because the term enforcing cybersecurity doesn't mean anything to me unless there's something to enforce them against.

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

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

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

Yeah, so I want to actually make a suggestion here, and it goes back to us talking earlier...I'm sorry, this is Scott Rea, again; talking earlier about the trust framework. And if we had a framework, a documented framework, that's essentially what would be enforced.

And I wanted to use an example of say e-Commerce in the Internet world. In order to enable that, there is a standard for how you implement security if you want to establish end-to-end security for doing e-Commerce and there are some standards that are published by the IETF, the Internet Engineering Task Force, that says these are the things that you need to think about when you create the policies that you're going to operate in and the technology that you're going to use and there's a standard format for doing that.

For instance, if we are going to utilize a technology of PKI, which, by the way, does have the ability to provide those three standards...three services...security services I was mentioning earlier. And the way that that gets implemented is you have a policy that says, these are all the things you need to think about and then you publish that in a policy document. And then those who are actually doing an implementation, create a corresponding document in the standard format that says, here are the practices we use to implement the policy. And then you have some external auditing body that verifies that yes indeed they are doing that. And then the accrediting body can take the attestation of the auditing body and put the trustmark on it to say that they're doing it.

And in this way, you have a set of policies that get published and you have a set of processes that implement those policies and that's how you establish trust, generally speaking, in a trust framework. And there are already standardized documents that...for creating these sets of policies and processes that you should be using. I don't think we need to recreate the wheel, we should leverage what's already available.

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

Yes. I agree.

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

I agree.

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

And speaking of not reinventing the wheel, the first two encryption recommendations, both say that ONC will work with OCR and industry organizations to develop standards in encryption...at rest standards and in transit standards, for data encryption...

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

We have standards.

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

We have standards and in fact, the certification requirements for EHRs already include standards for at rest and in motion. They point to the NIST FIPS 40-3, I think, Appendix A. So I don't understand what they mean by they're going to develop standards; do you know that Julie?

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

Um, okay, so for this one I think what we were trying to get at is more than just the standard that you had mentioned, but more of standards of how stakeholders and providers can actually implement data encryption.

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

Then that should be implementation guidance, not standards.

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

Yes. If the workgroup would like to comment in that sense, then that would be helpful for us. We all know that from stakeholder feedback we do know that a lot of the times they are saying that they don't know how to implement encryption and they need some kind of assistance or guidance from OCR or the federal government on what they should be doing.

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

Yeah, I totally agree and I think it should include both integration of encryption and the strength of the algorithm as well as key management. So we can comment about that.

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

Right.

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

Um, just, Dixie, this is Lisa; before we leave this slide, I have a question. I asked it earlier to Jeremy and Julie, but I'm not understanding why the out years in the roadmap have stakeholder input requested as placeholders when I know for sure that lots of folks in the industry provided comments on the out years and it seems as though that wasn't included. And I don't know if it's because it didn't map well to this chart or if they rejected the input that they got and are looking for something different. And so Julie and Jeremy, do you have any insight into that?

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

Jeremy, do you have information on that or...

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

Yeah, I tried to track some of that down for you, Lisa and what my understanding is that the feedback was incorporated in other areas of the roadmap. Do you have specific examples where we missed something?

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

Oh yeah, I mean I can give you examples. I think that there was a pretty thorough treatment in the HIMSS comments and others as well as the stakeholder comments from the meetings that I attended where we were trying to define end states in those years for cybersecurity outcomes. And it just wasn't expressed the same way as this is and so, it's just kind of curious to me to have those left blank. I mean, I can give you examples if you want me to look them up, but I would just refer you to the public comments and to the AI report, which I mentioned in my email.

I also wonder why, when we had the stakeholder meetings, I know that the roadmap sections do not limit themselves to actions of the federal government, but actions of the entire industry, levers within the industry, etcetera. And I'm wondering why this is just limited to actions of the federal government; is that a conscious decision?

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

Jeremy, did you want me to take that or...

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

No. It's not necessarily a thing that the federal government is the only stakeholder in a...for cybersecurity. Obviously we recognize and we state in the roadmap that this is a shared effort and so, going back to our general questions, where we specifically want that feedback. And if that feedback has been given to us before and it somehow was missed or lost in translation between point A and point B, please point that out and...

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

...I'll take this down...

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

...I would say that during the stakeholder meetings in the late summer, early fall, Dr. DeSalvo, Erica Galvez were present for the entire meetings, we focused a lot on a complete set of items that were across the industry as well as the federal government. So, that seems to have gotten lost. And again, I would refer you back to, in particular with this comment I'm making, to the Audacious Inquiry report from the stakeholder meetings because we worked very hard on possible levers and other things that were not necessarily federal government led, that could have an impact. It might be in the governance section, but I think it's applicable here and so maybe there wasn't the mapping made.

But I think...really, I mean I'll give Dixie some comments on this but I think there was a lot that was missed from the stakeholder comments and the industry input during the public comment period. And I really am concerned because it...I don't know if it's really that it was rejected or it was just not understood, but I think we're asking the industry to do what in some senses they've already done and it's not clear if it just...you didn't think it was a good idea, because it wasn't carried through here. But it seems unfortunate to have to dig up and give back the same input that we gave in the fall.

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

Okay, we can make a general comment to that effect, Lisa.

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

Yes.

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

Maybe you can write that up. The last two encryption were ONC will develop guidance to implement encryption policies, I guess that's encryption usage policies. And then the last one is ONC will work with payers to explore the availability of private sector financial incentives to increase the rate of encrypting, starting with discussions with casualty insurance carriers who offer cybersecurity insurance. What does that mean? The rate of encryption, is that like how fast you can encrypt? I guess that's the use of encryption? Julie, do you know what that means.

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

To increase the rate of encrypting, yes, that is to incentivize, for lack of a better word, if that is something that would be more effective to get people to do this.

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

So...

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

...and there are a lot of discussions about cybersecurity insurance and what they are doing in the space of making sure also that people are being secure and what those standards are as they write these policies. So that's where that came from.

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

So in order to get cybersecurity insurance, I would assume you had to implement encryption.

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

Right. It varies right now, I believe, from the discussions that I've had or been privy...yeah, my experience with that. There are no one standard adopted within the insurance sector with regards to what are the...

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

Oh, I see, so you want to get all of those in carriers who offer security insurance...

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

Right.

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

...to factor in the use of encryption into their rate structure or something.

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

Right, and if that is even wise to do.

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

Yeah. Okay, let me...we're getting up to public comment time, let me just go...quickly let me list these four recommendations I captured from the encryption part and then we'll go into public comment. One is to add key lifecycle management including key recovery and escrow provisioning. Two is to add governance. Three is Lisa's going to write up the ISAC recommendation. And the fourth is that the points one and two, recommendations one and two, where it says will develop standards should be will develop implementation guidance. So those are the ones that I captured. Did I miss anything?

Okay, I think...let me, before we go to public comment, let me thank you all once again for dialing in and for a very, very useful discussion. We really appreciate your contributions and your engagement here. Okay, let's go to 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 Collins – Junior Project Manager – Altarum Institute

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

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

We have no public comment.

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

All right, all right. Thank you all. I'll give you a minute back. Thank you very much...next time.

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

Thank you, my clock does not show a minute, but I appreciate it being done on time anyway.

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

Oh, okay. Next time we'll talk about section F. Thank you. Bye, bye.

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

Bye.

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

Bye.

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

Thank you.

Public Comment Received During the Meeting

1. 1. Page 59 of Interoperability roadmap talks about trust issues with Direct "The lack of consistently applied methods and criteria for both identity proofing and authentication has significantly hampered the exchange of data across organizations. "
2. Comment: One needs to include (not exclude) the smaller provider in solo practice in a rural area. Such a provider may not have the resources for advanced cybersecurity threat analysis and mitigation. The Security and Cybersecurity Infrastructure in a small practice will likely be less complex due to relative lack of resources.