

**HIT Standards Committee
Privacy and Security Workgroup
Transcript
March 17, 2014**

Presentation

Operator

All lines bridged with the public.

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

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

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

I'm here.

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

Hi Dixie. Walter Suarez?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Yes, I'm here.

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

Hi Walter. Lisa Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Here.

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

Hi Lisa. Chad Hirsch? David McCallie?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Here.

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

Hi David. Ed Larsen? John Blair? John Moehrke?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I'm here.

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

Hi John. Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Here.

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

Hi Leslie. Mike Davis?

Mike Davis, MS – Security Architect – Veterans Health Administration

I'm here.

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

Hi Mike. Peter Kaufman?

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

I'm here.

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

Hi Peter. Sharon Terry? Tonya Dorsey? And do we have Julie Chua on from ONC?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Yes, I'm here.

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

Hi Julie.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hi.

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

Before I turn it over to Dixie I do have one announcement that I wanted to share with the Workgroup. We are undergoing a few transitions to our Standards Committee members in the coming year, so Dixie Baker she has one year left on her term and we wanted to make sure that we have a Co-Chair of the group that will be able to help transition as Dixie transitions off of the committee.

So, with that I want to let everybody know that Lisa Gallagher will be our Co-Chair for the coming year. Dixie will still be our Chair, but Lisa Gallagher will be our Co-Chair to help us as we transition.

Just going forward we also want to make sure that our Co-Chairs are members of the Standards Committee, but unfortunately that means that we lose Walter as our Co-Chair, so I also want to take this time to thank Walter for all his help and support and let him know how much we appreciate everything that he's done as the Co-Chair.

So, a few changes and I'm not sure Dixie if you have any other comments, but I just want to thank you all for the tremendous amount of time that you provide to us to support this Workgroup and the committee as a whole.

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

Thank you, thank you, yeah, I want to thank Walter as well, I want to thank him for being a Co-Chair for a number of years now and I also want to thank him for agreeing to continue to work on our committee even though he'll no longer be a Co-Chair.

I also want to welcome Lisa, I'm very pleased that you'll be the new Co-Chair and I'm sure that the Workgroup will be going under great hands when I leave next year.

We've got a very good agenda today. The main point on the agenda will really be to begin our discussion of the NPRM, but first we wanted to – and let me tell you the schedule for that Notice of Proposed Rulemaking, for the April 24th meeting of the Standards Committee we'll be giving our review inputs on the NPRM for the security sections and we'll also give an out brief on the NSTIC Hearing that we just had last week. So, we'll spend some time this morning or this afternoon I guess talking about that as well.

We have two more meetings scheduled this week to discuss the NPRM, one on Wednesday and one on Friday, I'm not sure that it will take both meetings, but we've got them scheduled just the same.

As you'll see Julie Chua and her MITRE team have done considerable work in preparing for this discussion and I really, really appreciate all the work and time and effort that they've put in on it.

So, we'll start our discussion with giving some feedback on the NSTIC Hearing, a number of you were on that hearing I know and then we'll start talking about the NPRM.

The ONC is taking an approach a little different for this NPRM, a little different from in the past, they've created a special taskforce, I think they call it the Standards Taskforce and some of the people in our Workgroup are on that taskforce, it's a small taskforce that's doing most of the heavy lifting on this NPRM review, but they have asked us to look at the security parts of it. So, with that, does Lisa or Walter, do either of you have anything to add?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

No, Dixie, I think you've covered it.

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

Okay, then let's get to the discussion. Let me see. Next slide, please. Okay, they've asked us – and I believe as part of the materials that were distributed for this meeting I included the Excel spreadsheet that shows you there were a couple of review items that have been assigned to the Implementation Taskforce and some to the Clinical Quality Taskforce as well as the Standards Taskforce or whatever it's called.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hi Dixie?

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

Yes?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hi, Dixie, it's Julie, did you want to start with a little bit of the NSTIC discussion first or do you want to put that in the end?

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

Thank you, yes, yes, it just went to the next slide and it was NPRM and I – yes, I did, thank you very much Julie.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay.

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

Yes the NSTIC Hearing was held last week and Walter did a lot of the heavy lifting and preparing for that NSTIC Public Hearing so I also want to thank you Walter for all the work you put in on it. I think that work paid off, at least from my perspective, I thought the hearing went very well and I for one learned a lot that I didn't know before, especially how international it was and the role of the IDESG, etcetera, but, I'd like to hear some feedback from some of you? Walter you want to start out?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Yeah, thank you Dixie, and yes I think this was – I think we met the goals of the hearing which were primarily to understand where NSTIC is and then get an initial set of reactions around the applicability of NSTIC to healthcare and I thought that discussion went really well as well. So, from my perspective I think we met all the objectives that we set for the hearing.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Hi Dixie, this is Lisa.

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

Yes?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

So, I also agree that the hearing went very well and, you know, we had speakers who were able to answer the questions that we had as it pertains to the health factor. I think the pilots were also very illustrative for us and I think our task or things to think about going forward is, you know, what is the potential, if any, work that we can do in the standards space to really focus in on facilitating standards development where needed and looking at any challenges to interoperable solutions for healthcare. So, I think it left me with a lot to think about as we go forward.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

This is David, I've got some opinions too when we're ready?

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

Yeah, yeah, David?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, I enjoyed the hearing in terms of there being a lot of content but I came away a little bit with the feeling like I get when I read that people say, you know, why don't they just figure out interoperability, how hard could it be, which is to say that this problem is still awfully big and diffuse from the point-of-view of the specific needs that we have in healthcare.

So, I heard, you know, quite a bit of plea that they have more healthcare representation on the IDESG Workgroup or the appropriate clinical subcommittee. It didn't sound to me like they felt like they had enough and I certainly didn't hear a suggestion that there was enough input from healthcare.

And I also think that they're dealing with just such a broad array of capabilities that it makes me wonder that unless we really narrow down on some very specific healthcare use cases we will stay too diffuse to have much impact.

You know, on the other hand, I mean, that's kind of a negative view of it, on the other hand I was pleased to see that there seems to be emerging consensus around a new generation of standards to take the place of the older standards that we have in our current healthcare stack.

So, for example, several different people testified about OAuth and OpenID Connect as being, you know, robust enough for, you know, future RESTful approaches and other newer approaches. There were a couple listed that apparently are still emerging, but, you know, everybody kept coming back to OAuth and OpenID Connect so it seems like that was a bit of a consistency that I was pleased to hear that and given that our – the Power Team blessed those for pilot use is consistent with what we said there as well so that seemed good.

I was most interested in the testimony from the postal service who felt that they really still needed to have a central broker to make it all work and of course, you know, the original vision I think of NSTIC was to avoid any kind of central brokers. So, that struck me as an anomaly that was interesting.

I mean, I very much appreciated and understood what the postal service was trying to do but it just seemed to me to be almost antithetical to the vision, original vision of NSTIC and I would think that in healthcare the notion of a centralized identity broker service would be troublesome, even though I suspect it could be done properly and safely it's going to raise some concerns. So, I think we have a long way to go.

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

Yeah, you know, that – the post office kind of confused me because, I too, I thought it was more the objective was go for a more distributed kind of identity management.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Dixie?

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

And not for a central, for a hub like that, so that kind of surprised me to hear that as well yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

So, Dixie, this is Lisa, the way that I understood the postal service as well as some of the motor vehicle services were to make available some third-party credentials that could be used and leverage their identity proofing processes, but I'm not 100% sure on that, but that's the impression that I got.

And also, I think that this notion makes me think that there are some policy questions that might bubble up here too such as is it acceptable for a healthcare enterprise to leverage third-party credentials, you know, identity proofing and credentials they didn't do themselves.

And also, some of the discussion on anonymous and pseudo-anonymous identities and their use in healthcare. So, we know perhaps there at some point will be some, you know, meaningful discussion on what is acceptable from a policy point-of-view as well.

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

Yeah, I thought the post office one wasn't just for identity proofing I thought it was a hub for authenticating your identity as well.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

I think it was a third-party credential that you could leverage in combination with others, but I'm not exactly sure what they're proposing because I didn't see it used yet in any of the healthcare pilots.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well, it, this is David, what I heard them propose was they will broker between incompatible services to achieve the interoperability that the standards apparently aren't yet ready to achieve, number one, and more interestingly, number two, they will anonymize with respect to the individual service where the relying party was.

So, they would de-couple the IdP from knowing who all the relying parties are, which has, you know, that's a pretty powerful privacy advantage...

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

Yeah.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

If you trust the postal service.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Right.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Assuming you trust the post office.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

So, this is Walter, I thought I heard the post office approach that FCCX particularly was intended to be really a federal-based application that could be extendable into the private sector but I didn't get too much of a sense of direction towards that point of making it extendable to the private sector that, you know, FCCX is primarily a service for the government ID as I understood it, as an identity hub. So, that's an interesting –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, but –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

I guess opportunity perhaps or question.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

You know Walter, I think –

Mike Davis, MS – Security Architect – Veterans Health Administration

Walter, this is Mike Davis, I'd like to respond to that a little bit. So, the FCCX was initiated by GSA and NIST and its – you're correct this was initiated for federal agencies, but you've got to remember that NSTIC has the goal that the federal agencies will be the lead for this and establish, you know, take the lead for the private sector. So, I think FCCX should be looked at as an exemplar not as the federal government's solution to NSTIC.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

This is Lisa, and I also recall now the Health Workgroup or the Health Committee for NSTIC is looking at the FCCX implementation. So, that would imply some sort of connection to the private sector in healthcare.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

If we would use it, yes.

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

Well the post office is public/private, the post office is a – you know, I thought that was why they put it with the post office in fact or one of the reasons was because it's a public/private entity. So, it's kind of a bridge already.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah and this is David, the thing that struck me is that if they found it necessary to create the central service for the federal users then why would we not expect a similar solution to be necessary for private or public users, meaning, you know, he was solving problems it wasn't just an implementation choice and I took that to mean there are problems with the current state of the art in NSTIC that needs something like FCCX to be solved and that's, you know, I don't know if that's the proper conclusion or not but that's what I took away from his defense of the central hub that they built.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

I mean, the challenge is that it's one thing to do it for –

Mike Davis, MS – Security Architect – Veterans Health Administration

Well, he stated but in a privacy mechanism, but they also stated that there was a big problem with the N-Squared issue that otherwise it would require each provider to maintain their own federation services and be able to communicate with everybody.

So the centralized service, they had the privacy aspect by not allowing the identity provider to know who it's being connected to, but they also had the notion that there is – the N-Squared problem was being dealt with in the cloud rather than having to be done by everybody individually, that's a significant issue.

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

But the whole idea of a federated system is that you don't need a, this is Peter, you don't need a central authority with the standards written in such a way that the federation can work without a central authority otherwise it's not really a federated system it's a system that's been broken up into pieces but it's not really federated.

I like the idea of having a system where you can create that anonymity but I'm not sure it's necessary for all users, but there is going to be some system that's needed, and this is kind of a tangent, to connect the disparate systems that can't talk to one another, for example, in Direct, which is a much more immediate problem, since Direct is required and yet Massachusetts providers can't talk to Rhode Island providers because they're HSPs can't talk to one another.

So, there does need to be something on top of the federation to tie things like that together for now, but I think the long run goal should be a truly federated system with standards written in such a way that you don't need a central supplier.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is Leslie, and I agree with that comment. I think further there needs to be more efforts with regard to harmonization between NSTIC and the work that's going on in Direct and potentially there is some opportunity for some cross convening to be called with ONC because there is an immediate problem with regard to Direct. I also support working towards a federated model because just the – it's not scalable otherwise.

And then I did have a question on the post office from the consumer point-of-view it seemed there might be opportunity for a provisioning capability within the post office based on their comments and I hope that to be the case, especially for consumers.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, they didn't go into that, I was surprised.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I was too, because I thought that was the biggest value proposition they would have for the population.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah.

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

And I think they started on that like, I betcha, 5 years ago they started on providing that for the public, for the private sector, that kind of service, before NSTIC was even on the table.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

So –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

This is David, before we get way off subject, back onto our real subject I just wanted to comment on that Direct thing which I don't think has anything to do with improper federation that's just the fact that there is a turf war going on for who gets to decide what's trustedness in Direct and it's a political turf war battle that had nothing to do with the Direct standard at all.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thanks, David.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

It could be resolved in a heartbeat if they just decided to trust each other.

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

But if it's going to be required –

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Hey, Dixie –

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

To be used for Meaningful Use it needs to be – it's going to need to be legislated to be resolved if they can't do it themselves, this is – it's a horrible situation to say that there is going to be interoperable healthcare, Direct is required to do it and yet anybody is allowing a political turf war to keep this from working.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, I, this is David –

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

Maybe as a committee we should say something like that, that this needs to be – either they need to fix it themselves by, you know, the end of September 2014 or we're going to legislate it.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well, they're working on it, this is David again, but I think they know that they have a problem. The great irony is that Direct eliminated the incompatible islands of different protocols and replaced them with incompatible islands of different trust. So, I don't know if that's a step in the right direction or not.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

I just would like to say that we're going to legislate it is a term that we can't throw around very loosely. If ONC was going to regulate it, it should have been in the NPRM that we're dealing with.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And didn't –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Well, at HIMSS this committee did recommend that this be done many years ago and we were summarily told no.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is Leslie –

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

We recommended what? We recommended what?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

We recommended that ONC coordinate the issuing of identities for Direct.

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

That's right, yeah, yeah, yeah when we –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

So, it –

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

It was another NPRM that we reviewed, yeah, and we made a –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah.

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

And we made a diagram and yeah, that's right, yeah.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

The thing is –

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

It's heartening to hear but it's disheartening that it was ignored.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

–

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

It –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well, remember the big deal, the turning point was the NPRM around governance and that NPRM was, you know, basically soundly rejected by the community and the government backed off and said, we won't govern it in a top down way and so this is what we've got.

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

That's what John is talking about, David, that NPRM, the governance NPRM was the one where, that John was just talking about, where we made the comment that the ONC should be kind of a governance body, a public/private, there should be a public/private entity that does the governance for Direct. Remember that?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah.

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

We had the –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

But –

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

Yeah.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

But the overwhelming –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Dixie, we saw this coming.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, the overwhelming –

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

So –

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

Yeah, yeah.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

So, this is John, this is John Moehrke again, I do want to indicate though that this issue is really a microcosm of creating a federation regardless of the technology.

So, this example is in the Direct world but even in the OAuth federation world you still have a similar policy space which has to mix together a federation of trust. So, you know, ultimately it comes down to, you know, a set of policies.

The other point I would make is to not put too much into the postal service's perception of centralized. If you are an identity provider the world looks to you as if you are the center of the world that does not mean that your identities are not federatable with other identities. So, it may just be a packaging problem not necessarily an actual.

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

Yeah, I was thinking that when they kept talking about hub which immediately brings to mind a single hub, right?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yes.

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

But in fact you could have federated, you could have a federated type of a capability, you know –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Right.

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

It wouldn't necessarily have to be a single point of, you know, single point of resolution of everything.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Doesn't their discussion on the N-Squared problem argue the opposite of that? That their intent really is to be the central, the central clearinghouse.

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

I don't know.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

And I think the IdP, if the IdP has to talk to all the other IdPs then, yeah, you've got an N-Squared problem again which is remediable only by standards and then of course that's not sufficient because of the trust issue that John correctly pointed out, if you don't agree on trust then it doesn't matter that you know how to talk to each other, you chose not to.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, yeah, the point of federation is that you have a smaller list of things that you need to trust, very much like the DirectTrust.org, you have a much smaller bundle so it's easier to manage that smaller bundle, but ultimately someone needs to say, you know, for any particular perspective where the trust should come from and why.

But, you know, ultimately, and, you know, I think that does bring up, I think, you know, David your first comment which is, you know, there is so much complexity in here it would be great if we could focus the use cases on, well let's solve this particular problem rather than let's solve all potential problems that anybody could imagine in healthcare, because you get to a specific –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Dixie, this is –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Problem and it becomes far more actionable.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Dixie, this is Lisa, just a point of information, I do know that the NSTIC is considering, for their June plenary in Gaithersburg, Maryland at their facility, a separate half or full day sessions relating to healthcare. So, perhaps this is a way for us to engage with them more formally and, you know, we've got plenty of time to do that for the June plenary.

There is an April plenary that's on the west coast, but, you know, they are thinking about having a separate, you know, half day or a full day session just focusing on the healthcare and perhaps to John's suggestion that we encourage focus on certain use cases that would be, you know, important for us to move forward now.

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

Well, we've talked about – the planning team talked about, for the NSTIC Hearing, talked about having a follow on hearing that was just – that would be, not a full day like that, but, you know, maybe four hours or so, three or four hours that was really focused on healthcare. And, you know, if they're planning on a half day for focusing on healthcare in June it might be a good thing for us to move ahead and plan that hearing –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

And also consider if we want to engage in that session that they have.

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

Yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

And we can focus on our sector.

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

Yeah, yeah, yeah, yeah maybe we should talk to Debbie about that. Julie would you kind of reach out to her about that?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Sure, I will.

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

See what she knows about it. You said it was in June, right, Lisa?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yes it's in June. I can look up the date but it's –

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

Yeah, that might be –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yeah –

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

I mean it might be of – you know, of benefit to them as well if we could help them get some insight into this that could be presented at that meeting.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yeah, I mean, I think we should envision it as a discussion or a way to engage with them and to do so with, you know, and also drive participation from the healthcare sector so we can talk about working together.

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

Yeah, I agree, that sounds good.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

I wonder, Dixie, I wonder, this is David again, I wonder if there is any interest at all in a focused problem around the DEA and prescription control substances identity management and whether there is anything worth tackling there or is that such a hot potato and so complicated we would stay away from it, and, you know, what I'm getting at is, you know, if we can't solve, you know, federated reuse of that rigorously managed credential what hope have we in, you know, other cases and maybe the answer is –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Well, I think –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

We can't.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

This is Lisa, I think there would be some interest from NIST on that. I know there was a change made to 800-63 that addressed how identity could be, you know, shared or passed on or delegated in physician practices with regard to that and I know that it's a healthcare use case that they are aware of. So, it might be an interesting discussion to have.

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

This is Peter, Tom Sullivan and I were the ones that actually instituted that change 800-63-2 and, you know, we've learned that the only way to make any changes with the identity regarding controlled substance prescribing is through NIST.

DEA is not interested in what ONC or CMS has to say about this, but is willing to listen to NIST, so that was pretty successful. I agree that we should consider, if we want to make any changes or suggestions on that deal with it at the NIST level.

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

You guys – Peter, you guys initiated what changes?

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

The changes in 800-63-1 to 800-63-2 –

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

Oh, oh.

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

Which allowed for the hospital identity proofing and using a landline address things of that nature. We went up and met a few times at NIST with the people who were writing that, unfortunately they kept retiring or moving to the executive branch and passing it off to one another so it took an extra year, but, as we all know it did end up finally coming through.

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

Yeah, yeah, I didn't realize that you were involved in that. Good. Okay, shall we move onto – Walter and I will be putting together a summary and observations and topics for discussion with the Standards Committee on the NSTIC Hearing. So, if you have any topics that you want to make sure that we address, I've taken good notes here today, but do feel free to reach out to us either of us is fine.

Okay, so shall we move on Julie to the NPRM discussion?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Yes, sure, okay.

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

And are you going to lead this discussion at this point Julie?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I can do that, I can take over.

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

Yes.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay, let's see, so let's go back to the, I think it's slide three Michelle.

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

Yeah, that, yeah, I thought we –

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer
– Office of the National Coordinator for Health Information Technology**

On the assigned topics.

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

The one before that, yes.

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer
– Office of the National Coordinator for Health Information Technology**

Yes, okay. So, basically, what we did with the slides is we separated the requested topic for the Privacy and Security Workgroup and then there are some secondary topics that we might want to address and other traditionally topics that we might want to address too.

But for this slide, as you can see, these are the assigned topics for the Privacy and Security Workgroup, it's pretty much the minimal set and it goes through, you know, the authentication and the ePrescribing is here with regards to VA that you guys were just discussing on, your auditable events, the audit reports, the amendments and emergency access, automatic log-off, your encryption, integrity and accounting of disclosures. Next slide, please.

So, for the potential comment topics these are secondary topics that the Workgroup has previously commented on and/or are relevant to the Privacy and Security Workgroup. It includes Blue Button in there, VDT, your transitions of care, etcetera. Next slide.

Tertiary topics we identified as possible privacy and security implications but the Workgroup has not touched on these previously. Next slide.

All right, so for the general changes of the NPRM they are proposing to discontinue the complete EHR, they added some certification packages and added Non-Meaningful Use EHR technology certification, and some other minor changes. For solicitations for 2017 they added some HIT modules and specific settings certification.

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

I had a question about this when I saw this before, Julie, what do you mean discontinue complete EHRs? Is everything a module now?

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer
– Office of the National Coordinator for Health Information Technology**

Well, I – from what I read is they – we used to have a base EHR certification.

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

Yes.

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer
– Office of the National Coordinator for Health Information Technology**

Yes, so now they're discontinuing that to make it modular I believe, I'm not totally sure of that.

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

Well that – you know, what bothered me when I saw this is that a complete EHR was the only thing that required security certification the modules didn't.

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer
– Office of the National Coordinator for Health Information Technology**

Right and I think they do have some changes with the certification policy modules for the privacy and security criteria but it's not until 2017.

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

Okay. So, everything that will be certified will be a module, EHR module?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

That's right.

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

Okay.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

You know, Dixie, I think I heard Steve Posnack say at the HIMSS conference that there were some challenges with the term complete EHR and so they were phasing it out and that had a lot to do with terminology confusion in the marketplace. So, we might want to seek further clarification on that.

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

Okay.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay.

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

I'm sure we'll hear more about it.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yes.

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

Okay, Julie?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay, and actually to add onto that comment I do also believe that they were trying to get rid of the complete EHR because it was making it clear that providers who are not necessarily required to purchase a complete EHR if it's not something or if it's a functionality that's something that they're not using.

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

Okay.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

All right, all right, so if we go to the next slide, this slide just shows which topics have actual changes and which topics have requested comments for the 2017 edition.

So, if you look the authentication access control and authorization ONC is requesting feedback on the two-factor authentication for two use cases.

And I think to make it easier, Dixie, I'd like to do each topic one at a time.

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

Yes.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

All right, okay. So, the first one, if you go to the next slide, slide seven, is authentication, access control and authorization. Basically, with this one the DEA final rule has moved, the federal prohibition against ePrescribing and requires two-factor authentication protocol that specifically meets NIST LoA 3.

For the September 2013 transmittal letter HITPC recommended that by Meaningful Use Stage 3 ONC should move toward requiring multifactor authentication meeting LoA 3 by provider users to remotely access protected health information.

One other thing that the HIT Policy Committee suggested that the Standards Committee investigate is how would we test that recommendation for two-factor authentication in certification criteria?

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

I know a fair amount about this and I don't understand what the question is here. So, I don't know if other people on the committee are understanding it either, but could you go into a little more depth of what are they asking of us?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

There was one for 2017 basically ONC is trying to see if two-factor authentication can be or should be used for ePrescribing of controlled substances and remote provider access to EHR technology. So, those are the two –

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

I don't see what difference ONC's decision would make in terms of controlled substances since it's already required.

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

Yeah.

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

And the DEA has already shown that they don't really listen to ONC or CMS. So, we just need to say, is it scalable and comment on it, but I think that it's already required.

And frankly, as a physician who has to use it and knows all of its pitfalls the hassles of having to do it, I have to say that it's not a bad idea to require two-factor authentication and I think that over the course of the next 10 years we're going to see it used more and more as more people have access to it.

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

I see, you know, this recommendation, this is the one that it came out of the Tiger Team. The Tiger Team recommended two-factor authentication for remote access to electronic health records and I think that's what they're asking about.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well, this is –

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

Because the ePrescribing, I agree with Peter, I mean, the ONC doesn't have anything to say about that.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

This is David, I think this is the use case that I was proposing completely unaware that this slide was coming up next, which is to say if you have a DEA approved two-factor authentication can we demonstrate that this is also sufficient, that same credential, for remote access to the EHR and, you know, if it's an interoperability NSTIC kind of question. Do I need to have two credentials, one for my DEA and one for remote access or will one credential work for both?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Well, and I think –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

And its asymmetric, you know, because obviously there are some people that need remote access that don't need DEA but if you've got DEA credentials in your pocket why would you need another credential.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

I think that –

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

Well, it's a matter of the standard and it's a matter of the companies working together. Certainly, you don't need to have to different two-factor authentication it's a question of is your two-factor authentication, you know, coming from semantic and your hospital which requires two-factor authentication for remote access is requiring an RSA token that doesn't work with your semantic filter.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, but that's also not NSTIC.

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

Well, wait a minute –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

That's not NSTIC –

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

David, let's not get into a policy question here, we're really talking about certification criteria and standards. So, we're talking about –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

No but –

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

Certification of EHRs. So, are you suggesting that if they – if the product that's being certified includes a two-factor authentication mechanism that's already been certified by the DEA that that part need not be certified again?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

No, no I'm talking about that the certification would test whether there was interoperability of credentials such that if you have a higher than necessary credential from someone like say, the DEA, that's sufficient for a lower use case like logging in. So, it's the NSTIC test case exactly, it's interoperability of standards around validation through an identity provider.

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

Validation of –

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

Did you mean to say higher or did you mean say higher or equal, because clearly –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, good catch, I wasn't being that precise, just saying it, if you already have an adequate credential in your pocket can you use it and showing that this would work for use cases outside the DEA would be an interoperability of identity providers that would be a valid proof point if we believe in all that stuff we spent a whole day listening to.

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

Well, then the certification criterion –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

It would be you'd have to prove that you were consistent with some standard that would presumably be from NSTIC.

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

Or whatever –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, I think that becomes the problem, so this is John, John Moehrke, the problem that you have in – as soon as people say, I want two-factor authentication, is okay, what's the technology that you want to use, because, you know, there isn't a "standard" that says, this is the standard for two-factor authentication.

Now NSTIC is heading towards a service-based identity system such that the service you sign up with can be a two-factor authentication service or a single factor authentication service –

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

Right.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

You get back from the service knowledge about, you know, what kind of level of assurance that identity is at. If we had such a service there would be the ability to leverage that service under a set of policies but it's not just simply to say, you know, implement this standard and you will be guaranteed you will get two-factor authentication. So, I'm a little suspect that we have the standards we can point at today for universal implementation.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, this is David, I agree, John, this is the test case to challenge that NSTIC is doing anything useful. If we can't solve this simple use case with what they're doing then either they need to get going faster or we should quit paying attention to them, because this is about –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Again, I'll defend –

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

It depends on the use case.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I'm sure they can it just will be under a certain set of policies and unfortunately it's the certain set of policies that often – when they try to scale those certain set of policies to all potential policies is where things generally fail, but agree.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah.

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

Two-factor authentication is not just a simple use case or a matter of policy because the actual devices are non-standard, somebody maybe using a fingerprint reader, somebody else maybe using a crypto piece, somebody may be using a one-time password –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yes.

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

That matches up against a server that's internal to the vendor. So, it is more of a factor and there should be some sort of a federation that you can have your two-factor authentication authenticated by vendor one and allow vendor two, you know, to, you know, for example if DrFirst has a one-time password and you're using Epic in the hospital that there is some way for Epic in a federated fashion to hit up against DrFirst and say, yes this two-factor authentication validated, we trust it..

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, that's –

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

It's being sent from Direct.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah, that's exactly the premise of NSTIC is to enable that to happen.

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

All they're asking us – wait a minute, we're getting – I think we're going beyond what we're asking, they're asking.

Look under specifically there, all they're asking is should we – should ONC adopt a general two-factor authentication capability requirement, in other words, should an EHR product whatever they're calling it now, be required to support two-factor authentication in order to be certified, that's what they're asking.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

But, Dixie, the rest of that sentence –

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

Is it for 2015 or 2017?

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

Well, the answer is like “yes” or “no.”

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

But the answer –

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

For 2017 or for 2015?

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

This whole question is about 2017. The whole question is 2017.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Dixie, look at the line over specifically, it says dot, dot, dot, we could put compliment ePrescribing of controlled substances they are linking the two.

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

Which could, but the basic question is, whether we should support – that's what I just read, David, whether we should support – whether we should adopt, whether ONC should adopt a general two-factor authentication capability requirement for certification.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Which could compliment –

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

Right.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

So, are you saying that the –

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

– all the rest is good, it's speculation, but the basic question is should two-factor authentication be required for certification.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

But it gets to the point I was trying to make, which is it would be very difficult to measure whether a product has that answer and whether the implementation they've chosen is acceptable to all who would use it.

For example, as was stated, some two-factor authentication systems are based on a fingerprint reader, that's a physical binding to a fingerprint reader, some of them are based on smart cards like the PIV card that the DoD and the VA uses, others are bound to, you know, other technologies.

It is true that more and more you're starting to see them being bound to something that is not technology bound. So, the SMS message to your phone those kinds of technologies are not really going to bind you to a particular technology, but ultimately that becomes the problem is how – if it was a requirement for multifactor authentication what would be the technology that would have to be proven in the test bench.

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

Well you would have to be able to configure the system such that a single factor wouldn't authenticate them, they would have to be able – the system would have to wait for the second factor whether that second factor were external or a hardware device, or an external service, or whatever it was but you'd have to be able to configure the system so that a single factor wouldn't log you in.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

So, Dixie, this is Lisa, I mean, it seems to me that – going back to the simple question, if we stick to the use case of remote access to the EHR and whether it should be a certifiable requirement for 2017 it seems to be that, you know, we would probably want to say, yes and save the detailed discussion and know exactly what they'd require for later. I mean, it seems like it would make sense even –

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

Well, that's the second –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Just to support remote access.

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

That's the second question there, Lisa, the first question is whether two-factor authentication should be required for certification. The second question is whether the Tiger Team's recommendation is appropriate.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

So, why is a security group talking about a policy issue?

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

I don't – yeah.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

All they want to know is if the two-factor is required, that's pure policy.

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

I know, exactly.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Well, but what I'm bringing up is there is a technology and a standard's aspect to this.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yes.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Which is exactly the fact that there is not technology or standards that support this until you get service-based identity, which is what, you know, NSTIC is striving for.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

But, I think that NSTIC is talking about interoperable solutions. If you're just talking about remote access to the EHR from a provider, you know, maybe it's a little simpler.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Not really.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

And there –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Do I need to bind into my EHR technology the RSA type proprietary solution?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

I mean, I think –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

You know what –

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

Can I say something?

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

Yes.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Sorry.

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

Hi, this is Peter again, as you probably all know I'm tremendously in favor of something like this, but partially because of my strong conflict of interest as an controlled drug ePrescribing Company, but I'd like to say, if we could, to say that we believe that the policy is a wise one but we think as a Standards Committee we'd like to re-address this in a year when we know whether the standard is a viable standard based on the outcome of the NSTIC ongoing discussions.

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

Yeah, I don't –

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

And then reassess it in a year.

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

I don't –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

That makes sense.

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

I don't think we should bind it to NSTIC. I think what – I think you certainly can certify a product either requires a second factor or it doesn't or can be configured to require a second factor or not. I mean, that's been going on for years not just NSTIC. And then whether one of those factors needs to be NSTIC is a totally different question that isn't being asked of us.

I agree with David that whether this policy is appropriate is not a – that's not our job, but actionable, you know, ties back to the first question. Actionable –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

And isn't it, this is David again, isn't – I mean, we've had this debate a half a dozen times over the last three years and I think eventually it settles to the level of assurance question and NIST has defined those in a very rigorous way maybe not with quite the breadth that it should, but it sounds like with Peter's work he knows how to get NIST to even change their mind.

So, it seems to me this is a pure and simple policy question of what level of assurance is required for remote access and once you answer that then you go to the NIST documents and say, how do I achieve that level of assurance there's dozens of ways to do it.

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

But, they're asking us whether the policy decision is appropriate and actionable.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

So, if we keep it to that simple question I would say "yes."

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

Yeah, it certainly is actionable and I would agree with David, I mean this is the only time they've ever asked us to approve a policy.

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

I'm sure somebody will correct me if I'm wrong but there's a difference between level of assurance which is the identity proofing that's required to maintain a security and the type of security that's used is the level of assurance which has to do with, you know, how you obtain that, how they've identified you whether it's face-to-face or on line and how that's done and we're probably looking for medicine for a level 3 and then the type of identity has to do with how you get your token or whatever. You can still, I believe, require a level of assurance 3 to obtain a single factor authentication.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Correct.

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

Well, but –

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

So, the respondent would require level of assurance 3 and a two-factor authentication and frankly the DEA did a pretty good job of skirting some of the issues that NIST has about things like FIPS or FIPS level 2 where it requires you to match the identity for like a biometric against a database and some things like the 3D Lumidigm fingerprint can't match against that but the DEA said or it can be accredited by us as something that we accept and that was pretty interesting that they're able to get some Non-FIPS compliant devices, which are really better than the FIPS compliant devices acceptable for controlled drug prescribing. So, we may want to put in something to that level.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is –

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

The level –

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is Leslie and I just wanted to talk a little bit more for a second about David's comment, because I do think that LoA and functionality are tied up on some of the swirl we talked about earlier and having a place to come to agreement around what tasks have a recommended LoA associated with that and then cross reference that to then therefore what factor authentication might best practice have independent of whether that's a provider doing a real note access, a patient uploading data, a provider downloading data to their office.

I think that absent some cohesive recommendations around LoA and associated tasks and authentication recommendations this swirl will continue and we really don't have time for a lot more swirl. We have Direct required in Meaningful Use 2, we have the work that's being done in NIST and this continues to come up.

So, could perhaps one of our recommendations be let's get to some discussion and agreement, and endorsement around tasks assigned to levels of assurance and therefore corresponding authentication.

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

But level of assurance is a policy question that's not technology question.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But it's a little bit of both though Dixie because –

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

It says technology is required for each level but the level of assurance is a policy question.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Right.

Multiple voices

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I guess where I think that it crosses over a bit is because there is best practice for use of data that requires a knowledge and understanding of the standards that you're asking to support it and they're not easily extricable and so if we were to recommend that, hey, we've got some swirl going on here, we need to come to resolution, how would that forum be brought together and it should be a body of both policy and standards in my opinion.

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

I agree.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is not one or the other.

Multiple voices

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

This is Lisa, not to further complicate things but where the –

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

All of them are applicable.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Healthcare workers of NIST are working on some use cases that they think might justify some gradation of the level of assurance as well. I don't have the details, but I could inquire.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

It would be good to have that harmonized with the work going on in DirectTrust too.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I just think there's an opportunity for some rapid consensus to be formed around these issues to reduce the anxiety and to do so in a way that knows that although it's a simple use case today the numbers of people involved will get greater, so this should be a scalable approach.

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

So, what you're saying is there needs to be some discussion between the policy and privacy or policy and standards groups to decide on level of assurance for different –

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Dixie, this is Julie, I just wanted to interject that on the September 2013 transmittal letter it has been recommended already that by Stage 3 it needs to meet level of assurance 3. So, that has been already recommended.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

For a provider and not – but there are other levels of assurance that we've already got in place that it's been – for instance a patient for downloading data could be as low as a level of assurance 1, uploading data is still up for grabs.

So, there's just an opportunity I think to have this kind of a discussion that recognizes that there are different use cases that may have a scalable way and corresponding authentication.

And I have been converted on this because I have always been an advocate of LoA 3 for anyone participating, but I think that there is a gradation and it would appropriate to discuss. Absent that what we have is disagreement on different trust organizations and different marketplaces –

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

That is policy, Leslie, you're talking about –

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I agree, I agree, Dixie, I'm just recommending that absent that kind of quality discussion it becomes very difficult to have a meaningful standards discussion. So, how do we marry those two to have that discussion.

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

As Julie just pointed out, if you look on the slide at the top and Julie just read it to us again, the Policy Committee has already recommended in a transmittal letter that by Meaningful Use Stage 3 ONC should move toward requiring multifactor authentication meeting NIST level of assurance 3 by provider users to remotely access protected health information, they've already made the recommendation. They're asking us to either say, yeah that's fine or argue why it's not.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And further they're also asking if we say either – if we say "yes" they're asking how we would test that certification criteria. So, those are two asks.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Right.

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

Right, that's exactly right.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Which is the point I was trying to bring up.

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

Right, right, right.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

That if we put this in the context of a standards discussion –

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

Right.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

We can't just simply say, yes we agree with the policy but there is no way to implement it. I think they're asking can this be implemented from a standards perspective.

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

Well it can.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

The other thing I want to interject before we go too much further is whenever you speak of level of assurance we need to separate, there is a level of assurance associated with the issuing of the identities, there is another level of assurance associated with the authentication in this particular session which is the multifactor authentication. So, there is in person proofing is often a term used for issuing the provisioning of identities, that's one level of assurance.

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

And –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

And the second level of assurance is authentication.

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

–

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

So we can't just simply say use LoA 3.

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

I think you should check the NIST document, there is not a separate – they are packages and LoA is a package and each package includes a method for identity proofing and a method for authentication in the package.

You can't have LoA 1 identity proofing and LoA 3 authentication it makes no sense. They are packages and LoA is a package that includes the whole thing.

And LoA 3 specifically, that we're talking about, includes in person identity proofing and two-factor authentication. You can't unbound an LoA. NIST is pretty adamant about that and most assurance people are.

So, if we said – if we said we understand that's a policy question, how would you – is there a way to certify that technology supports two-factor authentication other than what I suggested?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

But it's a trivial question to say does technology support two-factor authentication so that can't be what they're looking for, right? I mean –

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

No, they're saying, can it be tested. Can –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

No.

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

Reasonably, is there a way to certify and I think that John's right they're talking about both the way to test it and standards to support it.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well, of course it can be tested. I mean, it's – they log in with two-factors every day to work, I mean, it's a trivial question that can't be what they want.

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

That is what they're asking.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well, we need clarification.

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

They're asking should they adopt, should they require two-factor authentication to be part of certification.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And the question of how would ONC test, it's testing the EHR capability that they are offering two-factor authentication so that they can certify.

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

Right.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Does that answer the question?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Well demonstrate it, demonstrate a two-factor login. Next question.

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

That's what I would say, that's exactly what I would say, demonstrate that you can configure your system such that one factor authentication won't get you in and two-factor will.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

And if you happen to have a DEA factor tough luck, oh, well, pocket full of tokens, ring around the rosy.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

That's because there's not a standard.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

I know.

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

Well, maybe that's what we – maybe that's what we point out that yes you can test it, but we – you know there can be a certification scenario but we know of no set – today we know of no established standards that, you know, we can use.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, the only standards you have are the ones you're describing which is a functional test.

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

Yes, yes.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I can functionally look at you doing something and see that you have functionally, this instance, you know, used two factors meeting the NIST 800, you know, 63 criteria.

It doesn't mean that your system actually does it right, it doesn't mean that you can support multiple configurations, it means you can support one. So, I don't know –

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

How about if we say, since most people use their ePrescribing to do ePrescribing on the same system we're talking about getting remote access to, to say that if the system has passed the DEA audit for two-factor authentication that will be acceptable, because most of these systems will have by that time passed the DEA audit for two-factor authentication and that is a much stricter thing than we're talking about.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

But this is – but Peter that's the problem that doesn't work for remote access to the system unless there is this interoperability that John points out doesn't exist yet.

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

Yeah, I think that those are basically the points that we need to make here, right there, you know.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah and –

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

That you can demonstrate it functionally, but I have a question for you Peter, is the DEA audit on a product or on an organization using a product?

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

It's on the product and the audit was unbelievably extensive where they went into the data standard, they looked at every aspect, at every screen, they make sure that the way that a user accesses the system is according to the final rule it is really specific.

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

Would you say if the product has passed the DEA audit that it would need to be tested further for this functionality?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

But now –

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
Well, the DEA audit isn't testing for remote access.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation
Right.

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
The DEA audit is testing for the product's ability to properly do the two-factor authentication.

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

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
So, you could say that the authentication used for the EPCS, you know, if that is the same thing used then it saves a lot of steps in terms of testing durability to take a two-factor authentication.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
So, have all the –

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
But why would they cheat on such a thing.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Isn't there options through the DEA certification where two-factor authentication is not implemented in the technology, it's done through –

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

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
A service provider?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Or a separate product, yeah.

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
But it's tested in the audit it doesn't have to be part of your program that's built there but it's tested in the audit.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Right but the third-party is the one that's doing the two-factor authentication.

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
Yes, but it's still you're testing that two-factor authentication in the audit and testing to make sure that it is appropriate.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Yeah, I'm not questioning the DEA's audit, I'm trying to expose what's getting tested.

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
What is getting – I mean, what gets tested in the audit is the integrated system –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Right.

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
That utilizes the third-party system. So, the two-factor authentication itself is being tested in the audit, it may not be written by the initial vendor but it's integrated into the system so it's being tested as though it were written by the initial vendor as a separate module.

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

Well, how about if we said this, how about is, yes they can be – it's possible to demonstrate the functionality.

Secondly, if the product has passed DEA audit that can be used to certify the product has two-factor for the EHR but doesn't address two-factor for remote access and then the third point is that the one that John has made is that given the number of approaches that can be used for two-factor for remote access, including the use of a separate service, we can't specify a set of standards to use at this time.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

And, you know, I have to just say the irony that we just finished spending all this time on NSTIC.

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

I know, I know.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

You know this is exactly what NSTIC is supposed to address and it hasn't so we need to be really clear about that, it's not ready for healthcare.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Well –

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

Do you think it – what about this is 2017?

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, but let me kind of throw in there David, they do have use cases that have been piloted that are equivalent to the DEA issue it's just that the DEA issue was not brought to them as a pilot program to work on and they're not trying to solve it on the scale of healthcare. So, you know, this gets back to the ask, which is that more healthcare get involved in NSTIC.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Right and I think, this is Lisa –

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

Maybe Lisa can bring this to the IDESG Healthcare Workgroup?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

I think the thing to understand is that NSTIC is not going to do every single use case for every single sector. There is going to be a requirement and a need for healthcare, you know, just as with any other sector, to come to the table to solve their specific use cases and so waiting for NSTIC to solve, you know, complex use cases for us is not, you know, the best scenario.

I think what I've been trying to do is to make sure that, you know, I don't hear anything in their principles or in any of the use cases that they are testing that are, you know, unworkable or conflicting for us, but I think we do need to come to the table in a way that, you know, brings forward either, you know, use cases we can deal with now or the challenging use cases that we need to deal with now, but expecting them to fall before us is really not – you know, it's more of a framework than it is, you know, solving every single use case.

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

Well, we can add that to our recommendation as well that this argues for healthcare's involvement with the NSTIC Program.

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

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

Okay, I think we have our answer. Do you want me to review it again? The components I have here that we'll make it read better, but the first is, yes, it's possible to demonstrate the functionality, the second point is that if the product has passed DEA audit that audit can be used to certify that the product supports two-factor for EHR functionality but not for remote access.

The third point is given the number of approaches that can be used in two-factor authentication for remote access we can't recommend a specific set of standards to use for this purpose. NSTIC and the – it's part of that one really, is NSTIC is not there yet, this argues for healthcare engagement with NSTIC Program. Anything else we want to incorporate?

Okay, I've got this written down, Julie we can go to the next one. Julie? Oh, there you go.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I'm here, sorry, I was muted.

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

Oh, okay.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

So, this slide goes over the auditable events and tamper resistance. Okay, let's see, so with this one we are asking for 2015 ONC is proposing a revised certification that requires EHR technology to present all users from being able to disable the audit log through EHR technology. So, that's the ask for this one.

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

Oh, I see, it's up there, the second sentence on the top, okay.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Yes. Because for the 2014 rule it was that only limited users could have the ability to disable but for 2015 ONC is proposing to just prevent all users from disabling audit logs.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Boy, talk about proving a negative, I just – this just seems silly.

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

Yeah, I think it does too, but –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

It's a policy.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I agree, it's a policy first off.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

And it's a negative policy that –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Yeah. I mean, you know, are you saying that there should be no human on the planet who can go in and screw up the code so that it stops logging, I don't think you could prove that.

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

Yeah.

Mike Davis, MS – Security Architect – Veterans Health Administration

I think it's a lousy policy any way, it's nonsense to say that we wouldn't be able to manipulate the audit log.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yes.

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

Yeah, yeah, of course anybody can change out that portion of the software or hardware and undermine.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

You know and can we say that the system already allows for preventing all users it's just that by policy nobody sets this to prevent all users that there is only limited users, right?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yes.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

I mean, currently the system is capable of preventing all users, if someone wanted to prevent – to have all users be prevented –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

What do you mean –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

From disabling the audit. I mean –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

Isn't that what they're asking, they want us to up the policy to say – and somehow certify that it should be impossible for anybody to disable audit and that's just not feasible.

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

That's –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

You can't certify that.

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

Yeah.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

I mean, it's pure policy.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

It's a question of just all reasonable effort so I don't think we need to – I think this is kind of crazy myself –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

So the key word is –

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

Can somebody give me an example?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Sorry.

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

Go ahead.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Well, I was just going to say the key word in the second sentence is that requires the EHR technology to prevent, in other words the system has the capability to the – the EHR technology has the capability to prevent all users today, right?

What it's saying here is that instead of having the capability it has to demonstrate that it requires the prevention of all users is that the way that this is to be understood –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

It looks –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

In other words is turning that capability to a required, that all users be –

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

No, there –

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

It looks to me like they're basically saying that you can't disable it using EHR technology.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Right.

David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation

So, the question you would have to then show every screen in your App and say, see none of those screens enable the disablement of the login, so there, we're certified, which would be silly.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

It seems we have consensus, why is it hard to move on?

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

Yeah, I don't –

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

The slide said that there were certain instances where disabling the audit log would be advantageous and I can't for the life of me think of a single one.

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

Well, and plus anybody who would disable it would be a system administrator anyway they wouldn't be a user. They're talking about prevent all users, what user could possibly disable the audit log?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Well, –

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

Well, it depends on the EHR, you know, a user might also be an administrator but why would you want to let anybody disable the audit log that kind of defeats the whole purpose.

Mike Davis, MS – Security Architect – Veterans Health Administration

For management.

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

Yeah, I think –

Mike Davis, MS – Security Architect – Veterans Health Administration

No, it's historically quite understood that if you turn all the audit logs on for some system you can take it to the ground and it won't be able to do anything. So, it's quite common to disable certain portions of the audit functionality and use that to monitor user access enhancing the amount of audit collecting on a user when you have some potential security situation coming to hand.

A lot of times audit is done in a statistical manner or where you log a single occurrence to a record and then turn the rest of it off, but if somebody is breaking glass or emergency access situations where they're exercising authorizations that require a higher level of audit then the whole audit system gets turned on.

This is a management function where system managers determine, based upon the policies for managing the requirements for audit, what things are on and what things are off. Usually –

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
So, you're talking about –

Mike Davis, MS – Security Architect – Veterans Health Administration

There is a version of both.

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

Mike Davis, MS – Security Architect – Veterans Health Administration

User selectable audit and audit that by policy should be on all the time. So, typically audit systems are configured where security events like a failure to log on isn't a mandatory audit event that's typically not configurable, but to say that system managers cannot turn off any audit is not a good security policy.

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

So, is that what you think this is saying Mike?

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

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

What do you think this is saying?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

That's what it's saying.

Mike Davis, MS – Security Architect – Veterans Health Administration

I think – I'm reading this as that, okay the original thing was some users, administrators, were able to manage the audit record now it sounds like they're trying to – and even if you buy a product, a commercial product, I think it's very hard to do this, but they're saying that prevent all users including administrators from being able to disable the audit log.

And remember, I mean, we're security people for heaven's sake, just because the audit log isn't functioning even doesn't mean that the security services aren't functioning, that encryption and authentication and all those services are running.

The audit services – the only purpose it provides other than, you know, analysis of events after they've happened is to guarantee that the services that you have are operating correctly.

So, I don't know what security goal is being met here, but it's putting a hamper on security people being able to properly manage the services that they're charged with.

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

Well, perhaps I'm misunderstanding this, but my understanding of the auditing is twofold, one is the security audit about access to the system and making sure the appropriate people are not seeing inappropriate parts to the system, but the other part has to do with medical/legal issues, did somebody go in and change something in a record and then not have that recorded in such a way that in the past the records said one thing and then the patient died and now the record says something else that it didn't say before and those seem to be two different audits. It could be I'm wrong about that, correct me if I'm wrong.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Correct. No those are two different audits. This is the security audit log, that is the medical records retention.

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

And what is this referring to this item? I'm in my car so I don't have the slide in front of me.

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

It's –

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

Is this referring to a security audit only?

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

Yes.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

It's the security audit.

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

Okay.

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

Yeah, in fact they point out –

Mike Davis, MS – Security Architect – Veterans Health Administration

That's what that assumption is, security audit, I mean, systems all have journals and other kinds of audits and they get all conflated with security audits, so –

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

No this is just the – yeah.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

So, we are all in agreement that this is not –

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

Well, have we answered their specific – their specific question is – we disagree that this is a good idea, we would leave it as it is right?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Agreed.

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

No change, okay. Pete's comment on the impact and potential unintended consequences of their – I think Mike has described those well, their proposed change and specific example for disabling an EHR technologies audit log is warranted.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Those were the same examples that were given when the 2014 was defined and I do believe there are examples that were given back then when the decision was made to allow, you know, have the ability to disable audit login.

Mike Davis, MS – Security Architect – Veterans Health Administration

I don't know of any policy change that has been promulgated since then that would, you know, cause us to consider such an onerous, you know, change to the audit management.

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

Okay, I captured that, that's good. Okay, so we're suggesting – okay, we're suggesting no change, we're not sure of the security goal but we believe this would hamper the security administrators from performing their functions properly, no policy change has been promulgated since 2014 that would warrant this change. Does anyone want to add anything to that? Okay.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Ah –

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

Yes, John?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, I guess the – I'm not sure whether this adds something but just to kind of put it out there, generally this kind of a declaration comes from the concern people have that the system administrator can thwart the system by turning off audit logging, going in and doing something nefarious and then going back and turning the audit log system back on.

The defense against that particular scenario is that the event of turning on and off the audit log is itself audited, that is not a negotiable audit event. So, you can see that the system administrator turned something off a period of time happened and then they turned the audit logs back on and you now, you know, can ask by policy –

Mike Davis, MS – Security Architect – Veterans Health Administration

Yes.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

What did you do during that period because we suspect these things changed. So, generally, this kind of an attitude comes from a worry about a risk that is already mitigated by, you know, something else.

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

But is that included in the certification now that the act of turning the audit log on and off is included in the audit?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Is auditable? Yes, that is in the ASTM specification.

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

Okay so it's already in there, okay.

Mike Davis, MS – Security Architect – Veterans Health Administration

Dixie, you might want to point out to pile onto John's point is that audit administrators are typically designated separate from other system administrators, it's a separation of duty function, so that's how the – what John said happens is that audit administrators can do their thing but the system administrators can observe those changes because it's still something that the system administrator can manage and see.

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

Okay, yeah – to look at, okay. Let's see what time – I think our meeting is over in one minute right? Yes.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Less than one minute now.

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

Yeah, okay, I think we've made some good headway here today and I really appreciate you guy's engagement in this, this is really valuable to us.

So, Julie, I've captured this I'll send you, I don't know if you have somebody there capturing these or not but –

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

We did too, but we can compare notes it's always good.

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

Good, yes compare notes and we'll get these into the next version or we'll get these into the materials you'll have for Wednesday. I hope you guys can join us then.

Anybody else have any concluding comments before we open it up for public comment? Okay, Michelle.

Public Comment

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

Operator can you please open the lines?

Rebecca Armendariz – Project Coordinator – Altarum Institute

If you would like to make a public comment and you are listening via your computer speakers please dial 1-877-705-2976 and press *1 or if you're listening via your telephone you may press *1 at this time to be entered into the queue. We have no comment at this time.

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

Okay, thank you and we'll talk to you on Wednesday.

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

Thank you everyone.

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

Okay, bye-bye.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Thank you .

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Bye-bye.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Bye.