

**HIT Standards Committee
Privacy and Security Workgroup
Transcript
March 19, 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? 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

Ed Larsen? John Blair? John Moehrke?

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

Here.

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

Hi John. Leslie Kelly Hall? Mike Davis? Peter Kaufman?

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

Here.

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

Hi Peter. Sharon Terry? Tonya Dorsey? Walter Suarez? And for ONC staff I believe we have Julie Chua and Kate Black?

Kate Black, JD – Health Privacy Attorney - Office of the National Coordinator for Health Information Technology

Yes, I'm here.

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.

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

And so just to let everyone know Kate Black will be here to help answer any questions related to the NPRM. And with that I will turn it back to you Lisa.

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

Well, thank you and good afternoon everyone. Our agenda for today is to continue our work from Monday's meeting of the Privacy and Security Workgroup reviewing the draft NPRM recommendations from the Policy Committee.

We have some items that we covered at our last meeting which we are going to recap and then we're going to proceed to go to the remaining items that we need to review for today. And at this point Julie would you be able to help us through the items that we need to cover today in the slide deck?

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

Sure, just to recap what we did on Monday was the authentication access control and authorization topic as well as the auditable events and tamper resistance. Michelle if you go skip to slide 7 please?

Okay, so with authentication access control authorization the main points that we were trying to discuss or have a recommendation on is basically that level of assurance 3 was in question and that's actually one of the things that ONC is asking in terms of Meaningful Use Stage 3 is requiring multifactor authentication meeting this level of assurance 3.

And if you look at slide 8 Dixie has pointed out one thing that she thinks the Workgroup should revisit is that the question of whether ONC should adopt a general two-factor authentication capability requirement as a prerequisite to certification.

She feels that the Workgroup has not addressed that question specifically and I also would recommend trying to see if the Workgroup is in consensus with the LoA 3 requirement for Meaningful Use Stage 3.

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

Hello, this is Dixie, I'm sorry I'm a few minutes late here.

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.

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

And this is Walter I'm also, sorry I'm late.

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

Oh, hi Walter.

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

Yes, hi.

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, I was just walking the Workgroup through slide 8 where you had a revisit of one of the recommendations made on Monday.

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

Do you want to –

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

Right two-factor general, yes.

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

Yeah, did you want to take over?

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

Yeah, as soon as it comes up here. I just wanted them to be aware that –

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

Yes.

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

Because our response said something about how there had been no change to warrant – let me see, let me bring it up.

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

Yeah.

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

There, there I brought it up. On the previous slide it says that – oh, this is the one about whether ONC should adopt a general two-factor authentication capability.

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

Yes.

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

Oh, this is a different one, I was going to my comment on the other one. This is they ask whether – they specifically asked us to comment on whether there should be certification criterion that all EHR systems should be able to support two-factor authentication, that's basically what they're asking with a "yes/no" answer and we really haven't answered that question.

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

Yeah, this is Peter, I think that, you know, there are new things on the horizon, but we should, at least temporarily, support the two-factor authentication with the caveat that as other things come out that show that they can be, you know, as secure, you know, but maybe simpler that we will revisit it.

An example is the 3D fingerprint that actually looks inside the finger and has multiple factors built into it, hardware factors to prevent spoofing, you know, that may be as secure as a two-factor authentication but it really isn't fully tested yet or really is available, you know, and affordable as we'd like.

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

This is Walter; I think it would be – I would probably be cautious about a general capability that applies across the board. I think there is situational need for two-factor authentication as in ePrescribing and then other one that they are considering is then beyond ePrescribing supporting this for remote access.

And I think if there is a general two-factor authentication capability requirement there is a question then as to whether organizations within or inside an organization everyone and who is everyone, that's the question, would need to have a two-factor authentication approach or whether this would apply only for certain areas such as ePrescribing, remote access, etcetera. So, that would be my caveat I guess.

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

So, you're saying there might be a subset of types of EHR functionality that might have that criterion but other types of EHRs would not? Because there's not –

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

Well, they're specifically calling out ePrescribing of controlled substances that's one functionality and the other functionality they're calling out is remote provider access to EHR technology.

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

And for the first one they already are required to do it.

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

There already is a subset of functionality that this would apply to.

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

And for the first one we're already required to do it.

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

Right.

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

Right.

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

Right, but we're not talking about an operational environment we're talking about the certification and they say, whether, ONC should adopt a general, they're asking us whether there should be a general requirement that EHR technology should support two-factor authentication which an organization could turn on or off, you know, that doesn't mean they'd have to use it all the time, it's just saying when you submit EHR technology should there be a requirement that your technology supports that should you choose to use it you know.

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

The answer has got to be "yes" because any EHR that's more than extremely tiny is going to have some users in New York State that will require two-factor authentication March 27, 2015.

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

Oh, that's interesting.

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

Yeah, except that –

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

They're requiring controlled drug ePrescribing which requires two-factor authentication.

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

Right, but those needs can be supported through, you know, through additional requirements. I mean, the Meaningful Use certification is minimal criteria not maximal or even optimal.

So, I mean, we would – it's not that we would be saying if you're in New York State you have to have multifactor, we're saying across the board, across large and small.

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

Okay, well then let me reword it, yes we should require two-factor authentication.

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

So, what do you say, John, what's your opinion about it?

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

So, my – I think this is absolutely a good goal. My concern, and I expressed it last time, is that we're the Standards Committee so we have to say what standard is this thing going to be measured against and I don't know of a standard that you can be measured against.

Yes there are some abstract standards like the NIST specification, but I get concerned, because I've seen it happen in previous years, where these things get put into the bucket of the jury decides and sometimes one vendor gets through with a success on their two-factor authentication and a different vendor fails because they've got a different judge and that's my concern, that's my only concern is that there isn't a consistent way to measure whether a product has good enough two-factor authentication capability.

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

And this is David, I share John's concern because the way this is worded as referring to a general two-factor capability that's – how do you test for that? What qualifies as a "general" two-factor capability? You know the DEA has been very precise, but that's not a general two-factor capability.

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

Well, just –

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

Well we said in our first part of our – and I did reverse the order of these because this second part, the second question really is dependent on the first, but if you look at the red print above there where it says that – we did say that this requirement – that the policy that the Tiger Team came up with is actionable, we said that.

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

So, you're saying just your so called functional test?

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

That's right.

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

As opposed to a test.

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

This is one of the few – this is Peter again, sorry to interrupt, actually I'm not I love interrupting, because I live to interrupt. This is one of the few things where there is a standardized testing for it it's NIST Level 3, it's not – NIST Level 3 is not perfect in every way but if we're concerned about the testing not being standardized all we have to say is two-factor authentication meeting NIST Level 3 and then we're letting NIST decide the testing procedure and everything which they've, you know, spelled out.

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

Yeah, but we –

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

But would this apply to every single, you know, EHR module and basic and everything or would it be –

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

Well, it doesn't mean it has to be used but the EHR has to be capable of requiring two-factor authentication if the practice decides that they want to do that, which is certainly more secure and that you're requiring a two-way level of NIST Level 3.

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

Well, but the problem with is that some modules might not – this might not make sense for some EHR modules to have a two-factor authentication element embedded in the module. They might do it, as I think someone else suggested, I think it was John, through an external application or capability but not embedded within the module itself. So –

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

But we don't have that as a requirement even in the first part Walter, we're saying that, you know, you could functionally test that the system could be configured such that it waits for a second form of authentication even if that's from an external – integrated with an external service it's waiting for that second form of authentication before it allows you to enter the system. It doesn't say, we haven't said that they both have to be integrated within the product.

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

Where did we say that?

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

In that print above, in the first, the first red type we said is actionable and we said, we specifically said the difference can be – given the number of approaches that can be used in two-factor authentication that they're not standards and we even talk about external devices and out of band services. So, we can't recommend a set of standards but we have said that functionally it can be tested.

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

And functionally is that NIST 800 specification that is a functional specification it's not a technical specification.

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

Right.

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

But this is David, my problem with the NIST specification is it lags market innovation by a couple of years as heard in our NISTIC testimony and if the only thing that passes is something that is explicitly mentioned in the NIST 800-63-2 I think we're doing the market a disservice.

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

Well, they don't let us –

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

And we heard complaints.

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

They don't allow us cite NIST Special Publications anyway as standards, so, you know –

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

Well, that's a good point.

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

It has to be guideline certifiers or something.

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

And if we say NIST Level 3 we're talking all the entire chain too not just a two-factor authentication step, right, so we'd be –

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

That's right.

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

Bringing in proofing and the like, which is not what they're asking us about.

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

But two-factor authentication doesn't mean anything unless it's been identity proofed properly. You can say you need a two-factor authentication you can buy the token down at the corner drug store that doesn't mean anything.

When we're talking about two-factor authentication we're not talking about NIST Level 4 where every user authenticating to the system has to have a crypto key, we're talking about NIST Level 3 which is more relaxed and, you know, likely acceptable where the user has to be identity proofed properly to a level of assurance, I believe of 3, and then with a two-factor authentication to log into the system.

And what I would require in terms of module is that I would say, it must be available at least for electronic prescribing, you know, and does not need to be used but must be available, electronic prescribing and logging into the system for clinical access. So you can still have – if you said it that way you could have the front office staff log in and only be able to see demographics, which is PHI, but much less and then with the two-factor authentication they could also see diagnoses and things of that nature.

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

But Peter –

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

Now keep in mind Peter that all the identity proofing, all that that's operational. All that we're talking about here is the technology capability that's all.

And were only asked – we're not talking about the identity proofing, we're not talking about 800-63, we're talking about when they bring a product in to have it certified should every product be required to show that it can support two-factor authentication.

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

And so in the first part we're saying that this is – it is actionable.

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

Yes.

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

But one thing is to say that it is actionable another thing is to recommend to be required.

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

That's right, exactly right and I'm hearing – the reason I'm not going forward is I'm hearing, you know, I'm hearing Peter say "yes it should be required" I'm hearing other people say "no it shouldn't."

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

This is Lisa –

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

Maybe we should say, no it should not at this time, because I'm hearing more people say "no."

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

Dixie, this is Lisa, I'm going to have to weigh in as "yes." I think that if you take it in the simplest statement that you made early on which is the capability to configure the system to require two-factor authentication then I would say "yes."

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

This is David; I'm going to side with John on this and say it's just too imprecise. We know that they're going to have to do it for the DEA and that's outside our control. So, there will in fact be the capability there whether we like it or not.

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

And remote access, and remote access.

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

Well, so remote access I think this just comes back to the risk assessment.

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

No, no. No, what I was saying is we already know that they'll be required for DEA and risk assessment or are you changing your mind on our first answer too?

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

Are you saying –

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

Well, keep in mind that not everyone, not all organizations are doing ePrescribing of controlled substances so that only applies to an organization that is choosing to do electronic prescriptions of controlled substances which is a fraction of all possible sites. That's just a point; I'm not saying it's necessarily a killer point.

The – and I absolutely agree with you Dixie that the requirement of a product having a capability does not in any way force an organization to use that capability. So, again, I'm not arguing that that's a problem.

But, I will point out and I haven't heard this one yet, the change to products requiring only simple authentication to all products across the board now must support two-factor authentication is a significant burden on the vendor community.

M

No it isn't.

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

Yeah, this is Peter, it's – the vendors aren't going to do anything that's not required for Meaningful Use these days because they have so much to do for Meaningful Use.

And I think it's – you know, we're talking about 2017, you know, a lot of years away from now and to say that a practice, you know, that wants to use two-factor authentication because passwords just stink and, you know, my practice is having this big argument, you know, now about how strong our password should be, we're requiring 11 characters for our passwords in my practice and that's for all staff and everything.

Passwords are so terrible to not tell the EMRs that they need to at least allow the practices to have that security with two-factor authentication since they're going to need the two-factor token anyway for EPCS and remote access and all practices by 2017 are going to be doing EPCS because many states are going to require it.

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

Yeah, Peter, but the problem – I mean, the problem is when you say at least allow it by virtue of putting it as a condition it doesn't matter it's required.

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

No it's required as part of the capability but when we –

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

Well, you're – but the vendors are going to have to build it.

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

I'm saying that the capability is there but the practice can turn it off, but we want the practices to have the option to turn it on if they want to be secure about their records.

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

Right.

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

They can always add –

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

The problem is humongous.

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

They can always add the functionality as a requirement of their purchase.

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

Right.

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

This –

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

The market –

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

Meaningful Use is a floor.

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

The EMRs are not building anything that's not required for Meaningful Use. I'm in the vendor community. We have 300 partners. The vendors don't do anything that's not required for Meaningful Use these days. The marketplace doesn't drive it, ONC does.

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

Well –

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

And I'm in the provider community and I have to argue that, you know, at the end if this is required to be built even if a provider decides not to use it they will have to pay it.

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

And –

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

Well, they'll have to pay for the development but they don't have to pay for the two-factor authentication, but they will for their EPCS.

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

But they –

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

Walter I'm a provider too, I'm in a 51 gastroenterologist practice and we have all sort of headaches, we're petrified that we're big enough somebody is going to attack us and we're going to get a multimillion dollar fine.

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

Well, but then you work with your vendor to solve the problem. Vendors often –

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

My vendor doesn't have time to do this kind of stuff, we're pulling teeth to get them to do any enhancements that aren't required for Meaningful Use because, you know, they're not a huge company, it's not a McKesson, you know, or Epic, you know, it's a GI specific program and they're pulling out all the stops to meet Meaningful Use. They won't do something that's not required for Meaningful Use.

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

So, adding something more to Meaningful Use is going to help you in what way?

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

Exactly.

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

Get them to do it.

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

I don't know.

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

And saddle them with more work than would be required if they just did it.

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

Yeah.

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

Because now they'll have to worry about how they heck to pass certification.

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

It's going to protect our practice from lawsuits from data breaches.

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

But then you –

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

If we so chose to make that, you know, a difficult step to use the two-factor authentication to login and by 2017 my practice is going to want to do that.

I mean, we were in a meeting last night of our IT committee which is 12 people and we're definitely heading in that direction and I know that we're not alone in this. And we're the doctors who are deciding this, they're the last ones who want to do two-factor authentication, but we know –

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

But you can choose a technology that can be plugged into your EHR to do that, but you don't need to require every EHR to do it.

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

You know, I think – here's a thought, now we're almost down the middle here, but I am, as you guys know, I'm pretty adamant about this Working Group not prescribing policy and I think that requiring that technology support two-factor authentication before there is a policy requiring it I think might be premature.

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

Yeah, so Dixie, this is Lisa, I wanted to add, you know, it looks like, you know, we're having a discussion on whether we should agree with this when it's not clear how it maps to Meaningful Use. In other words are we trying to drive the vendor market to what we think is best practices –

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

That's exactly what I'm trying to say. There is no –

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

Policy there that's mandating it. So, aren't we –

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

Hey, Dixie, Dixie, I might be able to make this quicker, can we table this and have a half hour call with the Tiger Team?

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

Actually, everyone, this is Julie, if you look at the slide there was a September 2013 transmittal letter –

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

That was about remote access, that was remote access, that wasn't about –

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

Yes.

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

The Tiger Team, three of us, I don't know whether Wes is on the call, but at least David and I are on the Tiger Team and I can tell you the Tiger Team has never discussed a policy for general for every EHR to do two-factor authentication we've never discussed that, right David? Did I miss some meetings?

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

No, I think that's correct, I think we were cognizant of the fact that it is inevitable that over time this will evolve as the standard, but we didn't see a need to make a policy for it other than the specific recommendation that it be strongly considered for remote access.

We wrestled with, you know, great difficulty with what the heck remote access means given that you use your phone in the hospital over the public network but whatever, so we basically stayed away from a high level policy statement that would require two-factor.

And I think the question here is we note that it's inevitable but does it need to be a part of certification because that means you have to define a test for it and that gets really complicated.

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

Even with remote access, now that you bring this up, even with remote access, I mean, if they're really outside the organization then they won't do two-factor within the EHR, they'll probably do one factor to get into the organization and second for EHR.

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

Yeah, I mean, we really wrestled that it's hard to define remote these days since everybody is using portable, bring your own device devices but, and so I think that's one of the reasons that we side-stepped it a little bit, but so I –

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

And if your EHR is in the cloud everybody is remote, right?

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

Yeah.

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

Yeah, yeah exactly, right.

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

I believe strongly in two-factor authentication being, you know, just the cost – it's the way you pass your risk assessment is you'd better demonstrate that you have that kind of security for authentication but I'm just leery of putting it in as a certification test given that there are dozens and dozens of different ways to meet the two-factor requirement and the market in that space is evolving constantly.

I mean, there's a, you know, there's a new company here in Kansas City getting great waves by using eye vein verification. I mean, it's pretty cool, it's pretty rigorous, but it's not in the NIST document and it won't be for years, but if an EHR vendor wants to use eye vein recognition and they can demonstrate that its secure why shouldn't they be allowed to do that? How would we test that that's adequate that's where I get hung up, it's John's point how would you certify.

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

Well, you wouldn't you would test whether the EHR waits for that second form of authentication whatever it happens to be.

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

So, what –

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

But how is it waiting? What is it waiting for?

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

And how do we do the functional test, is that – I mean –

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

You would show that you cannot login with just one factor that the system awaits an input from a second factor.

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

But, I'm saying from a regulatory point-of-view how is that captured? Is there – John made mention that we needed a standard to certify against, I mean, maybe this is an ONC question. I think all we know –

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

No, no read what we have up there, I think you're going backwards David. We've already said that you could only test it functionally there are no standards, that's what that, the red font, the upper red font says, that's what we said already.

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

So –

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

So, the certification criteria would be a functional type of –

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

Right.

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

Certification criteria.

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

Are we backing off from that too as well? Do we want to – I mean, we certainly can if you guys want to. Do we want to change our first and says it's not – it's actionable functionally but there – you know, it would be hard to specify a specific criterion or standards?

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

Dixie, what if – this is David again, what if we made a compromise and said, as per your point a minute ago, we believe this is fundamentally a policy question but if the policy should be declared that a general purpose two-factor authentication is required for certification we believe that only a functional test could be done because there are no relevant standards.

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

Yeah, which is a repeat of what we've said above that, that's what I think we should say, actually.

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

So, but I'm saying expand it to the general case. We think that it's –

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

I know, I know, yeah, I understand what you're saying.

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

Okay.

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

And I agree with you I think that's what we should say.

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

I agree too that sounds good.

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

Okay, that's what we'll say.

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

Yeah, I think I'm fine with that.

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

Okay.

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

Well make it unanimous.

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

So for our answer we're going to it's a policy question but – and then repeat, but can only be tested functionally.

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

But if the policy was to do a general two-factor authentication it can only be tested functionally.

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

Yes.

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

Well, doesn't NIST specify testing for level 3?

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

NIST is not a standard it's a special publication, we've never been allowed to specify NIST documents as standards and that one in particular is a special publication.

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

Is that true though Dixie?

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

No, they keep changing. They have waived on that one John I have to tell you.

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

Yeah.

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

Remember when we started out they were – they wouldn't even let us cite FIPS initially.

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

Yeah.

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

And they eventually said we could, so –

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

I mean, I think in this case it is factual that 800-63 is a functional specification, so it's an abstraction, but, you know, there are certainly are NIST specifications that are worthy in other areas just not in this one and, you know, I think we will see things change in the coming years as technologies like OAuth become more clear how to use them and that then gives us a pluggable service for authentication and authorization that then, you know, requiring an EHR vendor to implement support of OAuth as a service provider than makes this more actionable and testable at the technology level.

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

Yeah, when Blue Button Plus comes along. So, are you –

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

So, can I suggest also, just to Peter's point, that one thing that –

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

But wait a minute, wait a minute Walter, wait a minute I want to finish with John first because I want to make sure I get what he wanted, I'm sorry. John do you suggest – I mean, there certainly is nothing that says we can't suggest citing 800-63-2 are you guys suggesting that we cite that in the first part of this response? Is it –

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

Well, as we were proposing the text just a bit ago, yes, where we all said, you know, yes it's a policy decision if you do a policy decision 800-63 LoA 3, you know, is a functional specification that we can use, but that is, you know, is only a functional test not a technical test.

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

Okay, we'll add –

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

It's however we were wording it before; I think it absolutely fits there.

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

Okay.

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

I would just –

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

Would that –

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

To the top part we'll add it, to the top, the first red response we'll add it there.

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

But, Dixie and John, does mentioning 800-63 preclude more recent advances that aren't specifically listed in 800-63, the issue that came up in the NSTIC hearing that they run a year and a half behind the market. I mean, I don't want to cite them as anything other than as a "for example" but not, you know, it must fit one of their specifically enumerated technologies.

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

In my read of 800-63 it has always been a specification of abstract concepts of these level of assurances with specific terms, but my historic read of 800-63 would not have precluded the example you gave, it just would have required an assessment to put the, you know, the whatever you said iris blood vessel or whatever –

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

Yeah.

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

You know, there would have to be an assessment by the local group, you know, part of the decision group for that risk assessment that they did declare it as a – but if the NSTIC are saying this has actually prevented people then maybe I'm not reading it right. So, I do want to put that caveat out there.

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

So, my suggestion was going to be actually before I got interrupted, my suggestion was going to be that we can say that this, a statement saying, you know, this is fundamentally a policy question, if the policy decision is made to require this as a general two-factor authentication then it can be tested functionally and then add through standards such as and then cite NIST and period.

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

Right, right that's what we have.

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

I don't think that's what we have but that's what I suggest.

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

You're saying sort of "for example" as opposed to –

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

For example, such as, exactly. I don't think we have that, I don't see it reading this red statement, but that's my suggestion.

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

Well, I was taking – you can't see what I'm writing down, but I –

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

Well, if you wrote it than that's fine.

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

Yeah, yeah, I – and they can use it however they want to use it, because we've been – but that's what we'll put, okay, such as. Okay?

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

It might be helpful if we can see what you're writing but that's all right.

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

I know it would be, but, actually MITRE is also taking notes and I just send what I write down to them and they – okay?

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

Okay.

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

All right, let's go to the next one. And we will, Walter, we'll, you know, we make these changes and we'll send it by you guys again. Now this is the second – this is the one I thought you were talking about. Would you please go to the next slide, slide 10 so that we get the context?

In our response, this is the one about the impact of turning off auditing and we say, no policy has been promulgated since 2014 that would warrant this change. Then go back to slide 9.

And in the red font that MITRE has inserted there it says, in a 2013 report, this is new information, this wasn't here when we met on Monday, the Office of Inspector General recommended that ONC propose a revision to the certification criterion. So, that's what's prompting this recommended change.

And they said the change should require that EHR technology keeps the audit trail, audit log operational whenever the EHR technology is available for updates or viewing. So, knowledge of this does that change your answer on the next page that's all I'm asking?

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

That's a good bit more specific than the case that we were considering. We were sort of taking it as a blanket capability across all the system and this is talking about clinical users when the EHR is available for updates or viewing.

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

Right.

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

So, this seems like a reasonable policy but how in the heck would you certify it?

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

Yeah, this gets back to, I think David mentioned it last time, how do you prove a negative. How do you prove you cannot?

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

Yeah.

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

There's actually I think a little bit more text in the NPRM that helps us here as well, because in there they specify that through the EHR technology there is no way to turn off these audit events which then gets, you know, leaves some leeway for some of the things we did discuss last time which is that you have other administrative tools which are not, you know, the certified EHR tools, but, I'm not sure how –

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

You know...

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

Can you certify by an assertion, just an attestation? I mean, is that allowed in certification tests?

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

I think that gets at Meaningful Use.

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

I don't know.

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

I don't think it –

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

I know, I'm just saying what if –

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

So, if you turned off the audit log and it turned off the EHR that would be a test that you can't do it. You know, if by shutting down the audit log it shuts down the EHR clinical functionality as well you've proven. I mean, there are ways to test it.

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

So, Dixie, by saying, ensure that providers cannot do we interpret that to mean that clinicians that use the system or the entire provider organization, you know, where does the system administrator fit in?

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

I think it falls under all users.

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

Yeah.

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

Requires EHR technology to prevent all users, meaning everybody and anybody that is involved in using the EHR technology whether for maintenance, control, restriction, access or as a provider actually using it to treat patients.

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

Well, I'm looking at the text from the OIG and it said providers, so the wording was different than user.

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

Yeah and it specifically says, when it's available for update or viewing, so if the system is down for maintenance and no one has access to it then obviously you – they're not saying you couldn't turn the login off then or if you have to, you know –

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

Yeah.

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

Turn it off to clear the logs out because they got overfilled or something like Mike was describing. But, they're just saying that when the system is up for "patient care" I'm making that phrase up, but when it's up and running for patient care you can't disable it that's what they want us to say.

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

And it says providers too, that providers can't, you know, that –

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

Well, that was my question.

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

Yeah.

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

Yeah.

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

Yeah, versus administrators, we did have that conversation about –

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

Yeah, but so the provider gets on the telephone and asks his administrator buddy to disable it while he, you know, cleans up a mistake, I mean, that's – they're trying to preclude that.

So, if the system is up and running audits got to be running is how I read this. If the system is available for care audit has to be running.

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

That's right, so are there – would you change – how would you change our response?

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

This seems like a policy thing.

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

Our response is on the next slide, right?

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

Okay.

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

Yeah.

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

I think this is onerous and unnecessary and –

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

I agree with John.

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

I'm not sure how you test it. I mean, I think the current solution that's in the NPRM should be sufficient as a Meaningful Use floor.

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

So, should we just, on this response that's shown now, just change, just delete that sentence about no policy change has been promulgated?

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

Well, I think that's still right unless you consider the OIG report as a policy change. Do we?

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

When you say OIG report what do you mean is it the NPRM or the actual Office of the Inspector General?

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

Yes, can you see the slide there Walter?

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

The previous slide Walter, slide nine.

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

The office.

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

It has some new text that we didn't have when we were talking about this on Monday and this is from the Inspector General's report and I think Dixie my question still is there is, does that constitute a policy change?

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

Well, it certainly is a –

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

It's a recommendation for a policy change.

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

Yeah it sure is, yeah.

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

But –

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

We don't really need that one sentence in our response anyway if we don't want to change our –

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

Yeah.

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

You know, it just begs for them to come back and say, oh, the – you know Inspector General told us, you know what I mean.

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

Okay, so I would agree with that, because no matter what the Inspector General said we're saying this is not a good idea.

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

Yes.

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

Right.

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

So, we just delete that sentence, no policy change, just so that we don't – okay?

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

I'm not sure slide are you guys looking at, I mean, I'm looking at slide number nine and –

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

Okay, but our response is on slide 10.

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

Do you see red text there Walter in the middle?

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

On slide nine it says the Office of Inspector General –

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

Yeah, that red text that references the OIG report.

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

Now go to slide 10, please, and see we have a second sentence that says no policy change has been promulgated.

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

I like the point we're making on slide 10 of that the audit log audits itself in the sense of you could go back and verify that the audit log had been turned off –

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

Right.

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

During a –

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

I'm just asking if we just delete the sentence "no policy change" would that answer still be good for us?

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

You know I'm trying to make the case that I think it is good because as John pointed out auditing the audit log itself would allow someone to test whether the policy had been violated if it should in fact become policy that you never turn it off, that's better than, so you implement the policy, don't turn it off then you can verify if somebody broke policy by looking at the audit log itself. So, we could test that the audit log is in fact audited when it gets turned off.

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

Oh, I gotcha.

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

Okay.

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

In other words that's the test to prove the negative is you prove that the audit log captures turn on, turn off events and then you're covered if they want to make this policy or not.

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

Yeah, so what you're saying, let me restate it, what you're saying is through the current list of auditable events and the current restriction of changes to what's auditable to an identified subset of users this policy can be enforced and proven.

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

Yes, that's a good way to say it with the current rules, I mean, the current audit standard.

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

What policy can be – I'm confused.

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

The policy that you –

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

The OIG.

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

Yeah, the OIG policy.

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

So you want to make a statement that the OIG's recommendation can be enforced and proven with the capability already in the 2014 ruling?

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

Correct.

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

Okay, okay.

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

Yeah, so and if somebody wanted to, you know, say, I don't understand what you're saying is we're saying we don't think you can certify and prove that the audit log can't be turned off by a user during ordinary operation, we think that's the wrong way to think about, you should in fact think about it that the audit log itself will tell you whether it was turned off and that can be – that proves that you violated policy if in fact that is your policy. So, it's just moving it to a testable space which is fortunately already covered by the current regulation.

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

By the current ruling, okay.

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

Yeah.

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

I mean, the other things is really going back to the overall concept of we trying to focus on standards and not so much policy.

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

Yeah.

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

It seems like that's a more appropriate standards level answer, otherwise we will be actually recommending that as a policy this be decided. This meaning, you know, the fact that the audit log should not be turned off or able to be turned off that's a policy level decision.

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

Okay. Did we get this our recorders? I certainly did not. So, did the recorders get what we just now talked about? MITRE are you on the phone at all? Am I the only one taking notes?

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

No, no, no I'm taking notes Dixie.

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

Okay, could you read back what we just said? What you have we just said.

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

Hold on one second. Uh oh, hold on.

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

There's actually another way for that policy to be implemented with the current technology putting no user into that group that has the permission to turn off the audit logs, so there are multiple ways to do it. There is no requirement that this group can't be empty.

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

Yeah.

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

So, I would suggest actually we start this statement similarly to what we just talked about with the two-factor authentication that this is fundamentally a policy decision but that we believe that there are current mechanisms to allow to control the ability to, you know, disable the log and that there – you know that would be answer basically.

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

Well, we said we don't think you can test it, but that current technology captures the information necessary to enforce what OIG is recommending, that's basically –

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

Sure all those things can be added, but I was just suggesting to start with a similar statement as we started the two-factor authentication.

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

Yeah, yeah, yeah, yeah, right, right this is a policy decision and yeah. Okay, okay, I've got sufficient notes for us to move on I think I'll send these to you 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

Can we just go to the next one, thank you all. 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, so the next topic is audit reports and the highlight of this is if we are intending to use ASTM 2147 Section 7.6 requires that there are 6 types of access to patient records in order to be certified even if that certified EHRs need not have all 6 of these access functions to be begin with. So, basically the 6 actions are add, delete, change, query, print and copy.

What ONC is requesting is the sufficiency of this ASTM 2147 for 2017 NPRM. So, this is not for 2015 they're asking for comments for 2017 and I'm going to go through the 3 things that they're requesting, one is the query action is not a defined term.

So, ONC wants to know if one the ambiguity has caused additional burden or challenges to the EHR developers and how they have interpreted this term and if there is any industry knowledge related to any plans to revise 2147. So, I suggest we tackle that first question.

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

I can help you with the last part, I don't believe ASTM is looking to revise E2147, it just a few months ago was reaffirmed, I can tell you when, but – so there is nothing there. I don't know of anyone who is confused about what a query is.

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

Yeah.

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

So, you know, I think there – I have heard some people in the RESTful paradigm who are confused as to explicitly when I do a get, which has query parameters is that recorded as a query or is that recorded as a read? Because it's – when you look at REST as a technology REST is ambiguous as to whether that is a read or a query.

Now the reality is either one is fine, the important part is to record the fact that it happened and, you know, either way, even in a RESTful paradigm, either way you record it, records the sufficient detail. So, I don't know of anybody who's confused.

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

I wonder where it came from.

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

Like I said the only one I've gotten anywhere close to Dixie is the RESTful community with this paradigm of query versus retrieve, because you use the get –

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

Yeah, yeah.

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

Verb on both of them. So, do you follow the get verb which is read or do you recognize that there is a question mark in your read and therefore it's actually a query and you're just talking religion then.

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

And Dixie, I'm not sure why they would be asking us as to whether or not the vendors have had confusion or additional burden. I don't know that we can answer that.

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

Yeah.

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

I think they're asking everybody not just us.

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

Yeah.

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

I think that's one of the questions in the NPRM.

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

Yes, okay, so –

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

So, we can answer number C.

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

Yes, but for A and B might we just say, you know, we don't have any direct knowledge of that and the best source of that is the vendors.

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

Yeah.

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

Yeah and I mean there are some of us on the call who represent vendors and we obviously should speak up if we know of a problem. I don't know of a problem like John. I haven't done deep investigation and I can certainly ask around but I'm not aware that this has been discussed in our shop.

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

And as a blogger on the topic I would think I would have been asked a question.

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

Yeah.

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

I do have to correct what I said earlier, ASTM E2147 was revised a year ago, but it is not currently out for revision and there were no changes made at that time. So, there were no changes requested at that time, but it has been a year.

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, thanks. Okay.

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

Okay, so if we just say it's – what John just said, was ASTM is not currently out for revision and we are not aware of any problems that developers have encountered about interpreting query, we've satisfied the mail on that one. Should we recommend that just add a definition of query?

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

You know that's one of those where you – as soon as you start trying to zero in on the definition you find that you make a bigger mess than not.

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

Then just say, Dixie I think that if we go further through the list of questions we're going to see that they're asking us whether they should add that as a required action and so I wouldn't even – I think we should come back to that question after we answer 2, 3 and 4.

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

Okay, let's go to number 2. Whether ONC should establish a minimum baseline set of actions that EHR technology must always be capable of for the purpose of audit.

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

So, now they're saying can we – should we require that the EHR have the capability to do those 6 actions that then it could audit.

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

Or a subset of those 6.

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

Right.

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

Those are, those just like all the other actions are intended to be the list of, if these things are noticed within the context of your application you are obliged to record that they have – you know, the details. So, I mean, the whole list in that section is a list of auditable events.

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

Yeah, that's –

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

So, no it's not a requirement that you – that an EHR must have the capability to do additions, deletions, changes, queries, prints and copies.

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

I mean, I think, that's what they are asking whether ONC –

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

Yeah.

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

Should establish such a minimum set. My concern would be setting it up in regulations. I mean, we're now getting so micromanagement level, granular level of regulatory prescription that it's going to be very difficult to untangle some of these things as the standards evolve and so having ONC to establish such a minimum baseline set of actions for example which might be a subset of the six elements of ASTM seems to me that would represent a tweaking of the standards itself in some ways.

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

Well, it still –

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

Well, actually the other way we can go is for them to quit picking parts of ASTM because they specifically called only section 7.2, 7.4, 7.6 and 7.7. If they were to just simply say, ASTM E2147 these questions are answered in the specification and it's only, how long is it, 4 pages long or something like that? I mean –

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

Right, yeah.

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

I think that's even a better recommendation.

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

I do too.

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

Move it up rather than continue to granularly prescribe and specify regulations.

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

Do we know why they excluded the other sections, what was the concern?

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

I really don't know.

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

So, we want to say, no basically, they shouldn't establish a minimum baseline, but we also want to add that we don't think that they should granularly specify individual pieces of 2147 but should adopt it, E2147, but should adopt it that whole section on audit. There is a section on audit and there is another one on accounting of disclosures. So, that whole section 7 I think it is right? Section 7?

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

Yeah, section 7 is on audit login for surveillance purposes.

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

Yeah.

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

And by the way the 7.5 and 7.8 that they, 9 and 10 that they eliminated are in the specification identified as optional. So, in that case the reason why they surgically said 7.2 through 7.4, 7.6, 7.7 is because those are the mandatory ones.

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

Yeah, but if they just prescribe section 7 it would still be optional.

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

I know.

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

Yeah, I mean that's the kind of –

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

Yeah.

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

Random regulatory activity that it's just inappropriate in some ways of saying it.

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

Yeah.

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

Because it begins to just specify so much in regulation things that it becomes a very difficult cookbook to cook with.

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

Yeah, I totally agree with you, yes.

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

And is it – this is Peter, is it kind of policy to say you have to have all these different types of access as opposed to just saying that, you know, is that something that we should be even dealing with whether they required more types of access or not?

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

Well, that could be, that could be certification criteria, but it seems to me sort of backwards to take the audit trail and, you know, mandate functionality because it's required, because your audit trail needs to record it. I mean –

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

Exactly, exactly.

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

Yeah.

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

Yeah and, you know, the guess I'm going to go with is that what has happened is the certifying bodies have said, gee we created an audit test for print and this EHR technology can't produce that audit event, should we fail them.

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

Yeah.

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

And, you know, the answer is "no" well actually do they have a functionality to print, if they don't then no don't fail them.

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

Yeah.

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

Right.

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

Yeah, maybe we should look at the – well somebody should just look at the wording and make sure it says that if you have this functionality you should – you know, you should record it in the audit, but, yeah.

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

What I think they're saying in the however paragraph, the second paragraph on the first portion of the text is that basically, you know, EHR vendors have to document some of this and have separate documentation in order to pass the certification and I think the bottom line question of the transmittal letter from the Tiger Team to us is a key question to try to answer is, you know, whether we believe that it is still feasible to certify compliance using the prescribed ASTM audit log standard and I think the answer is yes.

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

Yeah, yeah, yeah and I think that requiring all this separate documentation, you know, that's a problem with certification, that's not a problem with the, you know, the process it seems to me.

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

Yeah, exactly it's a process issue not a standards issue.

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

Yeah. And as a comment we should probably say, yeah. Okay and then section 3 or question 3. Whether there are other actions that ONC should consider specifying in an updated standard that the current standard does not sufficiently address. Well, we've already mentioned a couple, right? Well, one, don't granularly prescribe pieces.

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

Well and they're particularly concerned about transmission.

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

It's going to be hard to capture that meaning at the audit log level.

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

Yeah, what is transmission in audit?

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

I, yeah –

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

Yeah, well transmission is a form of copy and if you were to go into some of the other audit log standards like Aetna there is an explicit mention of a transmission. So, this is a general purpose, you know, E2147 is general purpose it doesn't get specific.

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

But wouldn't you have done a read in order to copy?

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

Yes.

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

So it would mean you could get caught by the query.

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

It's just that it's not specifying the different actions that were taken read, copy, transmit in that specific level.

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

Yeah, that's a good –

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

No, I think transmission is not necessarily a copy either, I mean, you can – you know, you can transmit a Citrix image and you haven't copied anything you just looked at it.

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

Right, what if – you know, what if you could –

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

Yeah you have. Yes, you definitely have made a copy.

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

Yeah, yeah.

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

Well, you haven't made a copy of the file you've displayed the contents of the file. You haven't copied the file to the receiver.

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

Yeah, ask the EU about that. That is absolutely a copy.

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

But, so John –

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

It's not at the same level of detail, but when it comes to the act of disclosure it is a disclosure.

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

Is it –

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

Right, but we're not –

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

The question is John, because I agree with that one it's a copy, that one is a copy but the other one is a simply view that is across, a remote view which means basically I am "transmitting" the imaged information into my screen from the server in another site.

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

Yeah.

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

Right, so, you know, when you're dealing with these low level fundamentals add, delete, change, query, print, copy that is a copy, now when you put it into context it is a copy of the display of this document, so it's not a copy of the document it's a copy of the display of this document. So, you know –

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

But is that a transmission?

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

You can slice and dice but nonetheless at the fundamentals it's a copy.

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

Yeah, I was trying to distinguish whether that was a transmission or not, or involved a transmission.

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

And do we think it's an audit event?

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

I say no.

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

Practically speaking how would you do it?

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

Yeah, it would be very tough I would agree.

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

Yeah and I don't have 2167 up here, but I can't believe that they don't have –

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

Forty-seven you mean or 67?

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

Twenty-one forty-seven.

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

Yeah, 47.

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

Yeah, 47.

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

Yeah, I'm trying to get my –

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

So, we want to capture on number four no, number three no, is that right?

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

Well, the request is actually misdirected anyway because section 7 speaks about the content of an audit event, so when something happens who did what, when, where, why and what was the action they did?

So, the what was the action they did is not the list of auditable actions there is a different list of auditable events which gets to the thing we were discussing earlier in that an auditable event is, you know, to turn on and turn off the audit log. So, there is –

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

I'm sure – oh, yeah, audit functions are section 5.

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

Yeah.

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

Yeah, audit 7 is just content, that's – yeah.

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

Yes.

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

Like date and time of the event, patient identification, for the rest of you here, type of action, copy is there, print is there.

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

But now I don't think they called out section 5. I think they only called out those specific subsections of section 7.

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

Yeah.

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

That's why I say, again, you know, the list of what is an auditable event is in section 5 and if they would just call out the whole of E2147, all how many pages is it now that you have it open, it's teeny?

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

It's a total of 5 pages, but I think, but it includes like sanctions. It has audit log report, disclosure log content, see that's why they didn't – section 8 is disclosure log, but if they would just do everything except, you know, disclosure log –

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

What does 7.6 –

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

And sanctions they probably be fine. They have, for the rest of you, the sections of 2147 one is scope, terminology is number two or two is reference document, three is terminology, four is significance in use and then 5 is the audit functions in health information systems, six is principles for health information disclosure, oversight and paper and computer-based health systems.

I can see why they wanted some sections, but I don't understand – I agree with you John, I don't understand why 5 isn't there. Seven is –

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

What is 7.6?

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

Pardon?

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

What is in 7.6 that they call out?

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

That's the action that –

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

Type of action, type of action, additions, deletions, changes, queries, print, copy.

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

Those are the six actions that are listed.

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

Yes.

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

Well, yeah, parenthetically there are six, meaning there are six examples.

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

Well, they don't have like an IE or an EG they just have type of action and then they have –

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

Yeah.

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

Editions, deletions, changes, queries, print, copy.

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

So are we good on this response Dixie?

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

I think what we said is, we've answered no to number three and no to number four.

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

Okay

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

And did we answer the question from the Tiger Team as a yes?

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

What was the question?

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

The one on top, I did capture that it was a yes that the Tiger Team addressed, I mean, suggested that the HITSC address whether it's feasible to certify compliance of EHRs with the prescribed ASTM.

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

Yes, yeah.

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

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Okay, I think we're ready for our next one Julie.

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

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

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology
Okay, so this should be a little easier because there is no proposed changes.

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

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
We can argue about that too.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
That's debatable.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology
But we give you food for thought though so let's see, for amendments –

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

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

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Can you advance, there, thank you.

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology
Yeah, so there are no proposed changes from the 2014 rule, but we, my team we were just trying to get the Workgroup to think of two things if there are any related concerns, standards related concerns that ONC should be made aware of and in 2014 comments on the NPRM the HITSC indicated that their suggested changes would not prevent linking to an external URL. Is this an issue that you would like to bring up again for the 2015?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
So, they're saying, somebody on the Standards Committee said that the criteria were not – were unclear and not aligned with HIPAA that wasn't us right?

Julie Chua, PMP, CAP, CISSP – Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology
I'd have to check, but –

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Because I don't remember us ever saying anything like that.

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

Yeah, okay.

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

No.

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

HIPAA and –

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

I will check that.

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

Okay, the 2014 testing procedures do not test for the following to functions that we requested, capability to append a response to a patient provided information, capability of EHR to enable the user to replace existing information while preserving the original information.

So, does anybody – what did your team have in mind here? I don't understand.

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

We were just trying to see if you wanted to revisit some of the suggestions.

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

Requested functions?

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

Yeah, because –

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

So these were requested functions but they were not made part of the 2014 requirements.

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

I see.

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

And we're trying to see if the Workgroup would want to revisit that for the 2015 since there are no proposed changes from the 2014 rule.

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

So, this is where we could pick up some functions that weren't picked up for 2014.

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

That is correct.

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

Yeah, whether for example we want to say, we insist that number three –

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

Right.

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

That number three and four be considered to be added in the 2015.

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

No we said –

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

Well –

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

I sure don't remember, I don't remember, I do remember we discussed amendments but I don't remember this recommendation.

Test procedures don't test for the following capability to – so a provider – so patient provides something and this is a capability for the – oh, for the provider to amend –

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

Well, so a patient provided information and then they say we want to amend – I want to amend the information I provided you and so the provider or the EHR doesn't have any capability to –

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

Respond.

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

Respond to that request of an amendment of a patient provided information.

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

Yeah.

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

It's append though it's not amend.

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

Yeah, they're saying that the patient made a change said "hey, this is wrong, this is wrong" and then the provider can make a comment saying "well, the patient thinks that they did this or that this was the case but the reality in looking over the record that's not true."

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

So it's append, append.

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

So the provider can append it.

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

Yes.

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

And I think if we're going to have a requirement to do there should be a requirement to test it as well.

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

Yeah that's probably where we got the not aligned with HIPAA.

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

The not aligned with HIPAA I don't recall, because I think it was –

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

Pardon?

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

Well, I think HIPAA's always consistent that it's an amendment.

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

Yeah.

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

And the fact that you do multiple amendments or just simply multiple amendments you don't say the first one was an amendment and the second one is an appendment. So, I think they need to be consistent and then they wouldn't have a problem.

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

Yeah, but it's not amending a response, this is saying what Walter just explained, that the provider says "I don't think you have my weight right" and then the provider appends to that patient provider information, appends their response. They don't amend the person's response.

They don't amend the person's information they come back and say "I don't agree with you." So, that is an appendage to their patient provided information.

And HIPAA does, yeah HIPAA does allow you to, you know, say the provider comes back and says something that is kind of – so are those, three and four are those part of the certification criteria but there are no test procedures for them or are they just not functions included in the certification criteria at all?

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

I will have to –

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

I don't think they are –

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

Get clarification on that.

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

I don't think they are part of the certification criteria.

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

Yeah.

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

I think those were things that we, back in 2011, whatever 2012, when we were or 2013 when we were recommending things for this we recommended these capabilities, but I don't think they made it into the final rule for 2014.

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

Well, I don't feel strongly about either of those but do you guys?

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

I don't.

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

I don't either, recall the conversation.

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

I mean, I don't – it's a lot of extra work for stuff that they can do already.

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

Okay.

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

I agree, I don't think this is –

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

There's other important things to worry about.

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

Yeah there is, yeah.

**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

Okay. So, we don't propose any changes.

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

Okay, so the next one is the auto log off, emergency access.

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

Could you advance?

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

Yeah.

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

Oh, thanks.

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

The Privacy and Security Workgroup did not suggest revision to these criteria from the 2014 and ONC has not requested any comments on this.

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

So, while –

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

And then this is just a general question that we ask of all the topics that have no requested changes.

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

Oh, I see.

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

So, if there are any standards related concerns that the Workgroup wants ONC to be made aware of.

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

Okay, so it's just a, you know, are you aware, okay, just kind of FYI.

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

Yeah.

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

I don't know of any problems with the current state.

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

Yeah me either.

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

Does the standard differentiate between auto log off and auto screen lock? Because, you know, often auto screen lock is more effective.

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

It allows either of them, my understanding.

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

Thanks.

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

Okay.

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

Yeah, I don't think, I don't have any comments on this one either.

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

Okay, so no comments, okay. Next slide is end-user device encryption and there were no proposed changes from 2014, however there was a HIT Standards Committee comment on the 2014 NPRM that says key management is not addressed in any certification criteria, effective key management is critical to secure exchange.

Does the Workgroup feel there is a need to be more specific – to have more specific guidance regarding key management for this topic?

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

I think we have discussed that, but, so I think the – wasn't there a NIST specification that we wanted to point at for this?

Basically, the thing we want to prevent is a hardcoded key built into the hard drive encryption technology that is, you know, not changeable and therefore is not effective.

The problem is I'm not sure that all possible uses of encryption of data at REST can be so easily described.

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

Yeah, there's so many different ways to do that, I mean, from file encryption to, you know, whole disk software encryption, to hardware encryption, you know –

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

Yeah, but we really wanted to stay away from –

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

...

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

We really wanted to stay away from data at REST encryption or the concept of data at REST and that's why we changed it really to end-user device, because data at REST includes internal data at REST.

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

No, I think the reason it says end-user device is because that's what the final – the rule that came out from the Office of Civil Rights on breach safe harbor said that you needed to get the safe harbor for reporting breaches, you had to make sure that data at REST on end-user devices had to be encrypted, that's what they use, that's what they referred to so that's why it's limited to end-user device encryption.

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

Yeah, well, yeah it was the differentiated from the back end.

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

Yeah, yeah, yeah.

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

Well, from the internal system REST.

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

Right.

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

Data at REST that doesn't have to be encrypted.

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

That's right, right.

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

That's the point I was trying to make, yeah.

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

So, do we want to – you know, I don't feel a need for any more specific guidance does anybody else?

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

No.

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

Yeah, I think I – the only reaction I would want to give is based on someone explaining what is, you know, potentially problematic with the current stuff and I don't know of –

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

I think they just – that Julie's team just went back and saw that we made this comment previously.

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

That key Management is not addressed and so they're bringing it back to us and saying, this still isn't addressed, do you want to say it again, right Julie?

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 correct.

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

So, do we have a need to say the same thing again? There is no doubt that effective key manager is critical to secure exchange, no question about that, but a lot of – some key management is certifiable and a lot of it – most of it is not. So, it sounds to me like everybody is okay with saying no we don't want or need this.

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

Okay.

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

I'm okay.

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

It's almost time to the end of our meeting. I think Julie we'll just take up with the next slide the next time?

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

Yes, it's a good stopping point.

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

And is Michelle ready to open up the lines?

Public Comment

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

Yes, operator can you please open the lines?

Rebecca Armendariz – 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 public comment at this time.

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

Okay, thank you all very much for dialing in today and for your comments and for your help and we will – I'll just send my notes over to Julie.

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

Yes.

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

But if any of you want me to send them to you – the MITRE team takes my notes and combines it with theirs and/or Julie and her team and mine are pretty cursory –

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

Yeah.

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

But they make them more complete sentences and then they'll come back to us next time with, again, draft responses that we can read through and make sure they say what we want. Okay?

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 correct.

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

All right, thank you all.

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, thank you.

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

All right bye-bye.

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

Bye-bye.

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

Bye.