



**HIT Standards Committee  
Privacy and Security Workgroup  
Transcript  
May 23, 2014**

**Presentation**

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

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

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Here.

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

Hi, Dixie. Lisa Gallagher? Chad Hirsch? David McCallie?

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

Here.

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

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

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

Here.

**Michelle Consolazio, MPH – 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 and Vice President, Physician IT Services – DrFirst**

Here.

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

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

**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, MPH – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Are there any other ONC staff members on the line? Okay, with that I'll turn it back to you, Dixie.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

You know, Tonya Dorsey has left Blue Cross, Blue Shield South Carolina, so we probably should remove her name from that list, right Michelle.

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

Yes.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah. Okay, all right, there are two things – two main things that we're going to talk about today. One is, I wanted to give you the feedback that we got from presenting our recommendations on the NPRM to the full Standards Committee and I did send those out to you, the revisions, and that triggered some further discussion on their request for feedback on the ASTM audit, E2147 regulation. So that's one of the things we want to talk about. The other thing was that when we were doing – developing the applicability, the example applicability statements, it was part of our EHR module certification recommendation, we discovered in that discussion that there were several things that seemed to be missing in the privacy and security criteria. And so I mentioned this to Steve, and he said that – he encouraged us to make any additional comments that we wanted to make and so, I wanted to bring those up to you today, too, to see if we want to recommend some – they're not major, but they did come up in that discussion comment, so. With that, let's just dive in, whoever is controlling the slides, yeah, I think I just – I went over that, that's fine.

Okay. This is the solicited comments on two-factor authentication. Go to the next slide please. And the only change that was brought up by the Standards Committee was that they pointed out, rightly so, that this recommendation that's based on remote access. It was from the Tiger Team and it says that remote – that two-factor authentication is recommended for remote access to the EHR. And the Standards Committee – well, this group said that yeah, it is possible to test a requirement for two-factor authentication from a functional perspective, but that standards were lacking there. But the Standards Committee suggested we also point out that in today's environment, the term "remote access" may be difficult to define as it's situational. Like if you're within a hospital and you're accessing it over your mobile device, is that still remote access? That was one of the examples. And so the suggestion is that "remote access" be clearly defined. Any discussion of that? Okay, next.

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

Dixie.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Uh huh.

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

It's David, I was on mute, sorry. Do we think that it is possible to define remote access? I mean, do we want to encourage a bureaucratic attempt to define remote access?

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Hmm, do we want to encourage, what do you mean? Do we want to – words?

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

Well, what – are we suggesting that they proceed with this recommendation around two-factors but that they define remote access and if so, are we comfortable that that's achievable?

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well the policy isn't in the – in fact, I'm not sure – they were asked – we were asked two things, go back two slides, I think it is, whether – it says the one thing is whether the policy recommendations are appropriate and actionable. And that's really where that response – what that response is to, it's not really a response that says in the certification criteria you should define remote access, because the certification wouldn't define remote access, it would just say, can you do two-factor authentication, right, I think. And I think that that response is more of a response to the policy question. So are we asking the Policy Committee and the Tiger Team, yes, we probably are, to further define it in the policy statement?

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

Yeah and what concerns me is that I think we would discover on deeper thought that it's a continuum of risk and it's going to be hard to draw a line and say, on this side of the line it's not remote access and on this side of the line it is remote access. And therefore, I don't know, I'm just worried about tossing the phrase remote access back and saying, go set up some rules to define remote access –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well the Tiger Team –

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

– because I think that's –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

The Tiger Team came up with that, so if we make a comment, it'll come back to the Tiger Team. So, you and I both sit on the Tiger Team, are we going to be able to come up with something reasonable?

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

Yeah, I mean my concern is that they'll come back and say, that's a technical definition, you tell us what remote is, and it'll come back to us and we'll have to scratch our heads and say, gee, that's kind of hard. I mean you pointed out that a cell phone within the walls of the hospital is one thing, what if that cell phone has been credentialed to access the hospital, is that a different use case.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah.

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

If that same credentialed cell phone is used from the golf course, does that make it different? I mean, it's just going to get so slippery. I don't know, John, what do you think, this is the kind of stuff you think about a lot more than I do.

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

Yes, this is John. I very much agree with you David and I feel bad that it's going to be sent over to the Policy Committee where you guys have to come up with the answer.

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

Yeah.

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

I only get to sit here so, I – there really isn't, as far as standards, a good differentiation either and I liked your example of a cell phone. I mean my corporate issued cell phone knows how to connect to the corporate Wi-Fi using strong authentication. So is it then not a remote device in that case, because it's using the Wi-Fi –

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

Right.

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

– and the applications on the cell phone really have no idea whether they're on Wi-Fi or they're on AT&Ts LTE, they really don't know.

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

Yeah, that's a good point, the apps wouldn't know even if the device was smart enough to do the right thing.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah –

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

I'm not sure there is a good answer, but I think it is useful yet, for us to push back and say, by the way, the word remote is not clear.

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

I think you could maybe – this is David again; you could maybe come up with a set of kind of parameters that affect the risk –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Right and –

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

– and say, use your judgment about high-risk settings considering these kinds of parameters. So, access to a hard-wired terminal when the person making the access is under the observation of other authorized users is a lower risk than access to a hard-wired terminal when there's no one watching, those kinds of things that affect a risk assessment. But I don't think we're going to come up with a clean

definition of remote. I think you guys talked me out of that, I made the naïve assertion that if you come through the firewall it's remote, but I think that breaks down.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, I think so, too. So go to the next slide and see what we said here. From a policy perspective we would not that today's environment "remote" may be difficult to define, as it is situational.

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

I mean, maybe we should rephrase that last sentence there in red to say, we would suggest that remote access be replaced with a risk-based assessment that takes into account the situation, or something like that.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, I like that.

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

I certainly like that better. I'm not sure it really makes it more measureable from a certification perspective, but certainly –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

– think we're talking certification at all because the remote business has to do with the use of the capability that's certified. I think it's totally a statement with respect to the policy because the certification is going to be, can you do two-factor authentication. So, Julie, did you get that, are you taking notes? Suggest that remote access needs to be replaced with wording that refers to relative risk or something 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**

Yes, and if I may just pose this question to the group, in line – because I agree with what you guys are saying, but in line with what you are proposing, because it's true that it is a risk-based assessment of what is more of a risk and what is not. But I think in the response we may want to say that if you agree, as a group, have a definition that's an industry definition of remote access. Because if we don't have a defined definition of remote access and we just say that it is situational, it is organizationally defined, then it would still be difficult – it's going to be like a cycle and what I'm trying to say is –

**M**

(Indiscernible)

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

– we should have some sort of concrete recommendation.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well if we just – I don't agr – I think that if we refer to their risk assessment, they all should do a HIPAA risk assessment, and they're required to do that.

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

Um hmm.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

And I – it's reasonable to just reference the – based on their risk assessment.

**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 Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Because I do think it's impossible, and that's saying something, to really come up with a clean definition of remote access at this point. I mean heck, you can even have a classified VPN from a mobile phone in this day in age, it really would be impossible. So I'd like to say something that refers to their risk assessment and I think that's the right thing to do. Okay, next slide.

This one has to do with accounting of disclosures and they – what they did, in that NPRM they're proposing to drop complete EHR – the certification of complete EHR and references to complete EHR and they also are recommending that all optional requirements be dropped out of the – no, the optional word be dropped. And so they ask us if we had any problem with dropping this with respect to the accounting of disclosures requirement, which is optional. And so we said that yeah, we agree that it's premature to include accounting of disclosures. We said that – let me see – the PSWG agrees with ONC's recommendation to remove the optional designation associated with accounting of disclosures criterion it's no longer necessary with the elimination of the complete EHR concept.

**M**

Yes.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, let's go to the next one, which is going to be a little harder. This one is the audit reports and all of these questions, I think all of them have to do with ASTM E2147, which is the standard that specifies audit, it defines audit and it also defines accounting of disclosures and it spec – has one section that relates to audit and another section that relates to accounting of disclosures. What they're asking is, section 7.6 – section 7 has the number of criteria relating to audit and section 7.6 has a par – in parentheses a number – I should have brought my 2167 – 2147 up so that I could show you. But it has a number of actions in it that are not in – they're in parens but they're neither an i.e. nor an e.g., they're just a number of things that are listed. Let me see, I can tell you what they are, I can bring this up pretty quickly.

Okay, here's what they are, and section 7.6 says, "The type of actions" and then in parenthesis it says, additions, deletions, changes, queries, print, and copy. And then it says, "Specifies inquiry any changes made with a pointer to the original data state and a delete specification with a pointer to delete information." This is – this whole section 7 is about the audit log content and these are – and each of the sections in there specify minimum data elements. So this data element is the type of action. So, what we were asked is whether to this list, this list of additions, deletions, changes, queries, print and copy that they should add – whether they should add transmissions. That's basically what they're asking.

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

Yeah –

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

Yeah, this is John.

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

Go ahead.

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

I certainly tried to explain that that is what a copy is, unless you want to get more explicit and say it is an export or an import. So, I don't mind them being more explicit, but a transmission shouldn't necessarily be seen different from a copy.

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

Or from an audit point of view, even a read, because you can't tell what –

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

Right.

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

– happens with the other end of the read.

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

Right, that's –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well that's, John, that's what I said in my response and you disagreed with it. I said a transmission is the same as a copy and you said, no, that's not true.

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

(Indiscernible)

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Go to the next slide with the –

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

I'm not sure I was – I don't think I was responding to that.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

See, our original response was section 7.6 specifies the types of actions to be included in the audit trail and should cover any type of action taken within an enterprise including transmitting a record within an enterprise, which would require a copy. That's what we said and that's what you then took exception with. Transmissions to outside the enterprise are covered in section 8, disclosure log content, but accounting of disclosures currently is outside the scope of EHR certification so section 8 should not be added at this time. So that was what we put forward and that's what you had an exception to. You disagreed that it would require a copy.

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

Yeah, the exception is to the second sentence, not the first. So what I was excepting – what I was having a problem with was the EHR typically cannot tell whether one copy is for non-disclosure purposes while a different copy is for a disclosure. So I think it's the second sentence, which we're saying –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Oh, I see.

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

– I realize you’re saying that it’s outside the scope, but it’s not even something that the EHR can necessarily tell.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, I agree with that. I agree with that, yeah. So if we –

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

So I would just simply stop at the first sentence.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, I’d be fine with that, anybody else –

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

This is Peter, unfortunately, I got another call and so I missed a lot of the discussion, but if the EHR did know whether it was internal or external, would that be okay to only have to log it if it was external –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well if it’s external, it would be accounting of disclosure, though. It would –

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

(Indiscernible)

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

– by definition be accounting of disclosure.

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

It’s not a disclosure if it’s internal.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Right.

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

Right, but the – what we’re speaking about here is the security audit log and the security audit log needs to record all copies, period. It’s the additional use of the audit log for creation of the accounting of disclosures that would benefit by knowing that this copy was an internal copy and is not a disclosure.

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

Got it.

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

And this other copy was an external, and therefore should be included in the accounting of disclosures. So –

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

That makes –

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

– again, keeping just to the question asked, we should just point out that a transmission is simply a copy in the context of that particular line item in the ASTM.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, I agree. I'm fine with deleting that second sentence; it goes beyond what we've been asked about, anyway. Okay. Okay, next slide. Let me see – I'm switching between the screen and – okay, next slide. This is still more – next slide. I think we've resolved this one. Next slide.

Okay, this one – now we get into these other three things that we brought up when we were discussing the applicability statements. And the three things were that the authentication criterion addresses the authentication of people, but not a software. The second one is that the automatic log-off says you should automatically log them off and doesn't that intermittent level of the screen lock. And the third one is that there were no general encryption requirements. So, we'll bring each of these up in turn. Next slide, please.

Okay, in the main bullet there, she's listed what it currently says, which is, it's called authentication access control and authorization. Currently says, verify against a unique identifier, user name or number, that a person seeking access to electronic health information is the one claimed. And the – what we have here is that we note the need for authentication to extend beyond persons to software servers and we recommend modifying this language to include servers that are seeking access to EHR – to electronic health information. And the example is to verify against a unique identifier, user name or number, that a person or software server seeking access to electronic health information is the one claimed.

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

You may want to say, software application or server, because sometimes you want to authenticate a client, not just a server.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, well, you know what occurred to me, should that just be entity?

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

Well, that's essentially – we're now reinventing the word entity, so an entity is a machine, a software, a client or a human. So, we're –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, you're right it's mixing things. Okay, so a software application or server.

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

Yup, and in both places of that paragraph, right, there are two places.

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

And this is David. Do we need to be so picky as to add notions beyond user name or number for the cases of servers, because it might be a shared secret or a time-stamp token, secret token? In other words, the servers aren't going to simply impersonate a person, they're going to be authorized through some other unique identifier method, typically.

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

Right. Do we need to say software server or virtual server since although medicine is lagging the rest of the industry, or other industries, virtualized servers and using these cloud-based systems is really taking over relatively quickly?

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, but they're still software.

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

Yeah, I would –

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

Yeah, they're still either an application or a server so, whether it's virtual or not.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, they're all –

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

I wouldn't think we need to add that. I think to David's question, I kind of cringed when we got to the e.g. as well, but since it was an e.g., I didn't get too much more around that.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

We could change number to identifier.

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

Yeah.

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

Well, we already have the unique identifier. Oh, I see, so you're saying by user name or identifier.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah.

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

And –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

So what would you put instead of number there, David?

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

Well I was going to, I mean, John's correct, it says for example, so it's not, it doesn't have to be a comprehensive list, but it just jumps out at me that a naïve person could read this and assume that servers are always being proxied to individuals when in some cases they aren't. They are authenticated through some other mechanism like a token or a shared secret.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

But that's –

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

So I just –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

– this is not talking about the authen – the verify is the authentication part. The unique identifier is this part, its unique identifier, that’s not the authentication mechanism, the token; this is what you use to identify them. So, you might use an IP address or, you know –

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

Hopefully something more robust –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

– this is the identifier, not the –

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

– than that. I mean I think it’s really –

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

Yeah, sometimes it – usually looks like a DN or a fingerprint or it is some type of unique identifier, which is what it was more normatively saying, so I didn’t worry too much about it.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, I think.

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

Yeah.

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

I think the e.g. is kind of there to link the more technical term of unique identifier to a more colloquial term like username. So, I’m okay with that part of it.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, let’s just add software application or server in both places and I think we’ll go with that.

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

I’m okay.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, this next one is the automatic time-outs. You’ll recall that we talked about how this one now says prevent a user from gaining further access to an electronic session after predetermined time of inactivity. So there, it’s termination of your session entirely, so it doesn’t really address that intermediate step where you just lock the screen. So the suggested wording is automatic time-out and log-off, automatically lock access to the application after a predetermined period of activity and then automatically log-off the user after a longer, sustained, predetermined period.

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

It’s still awfully cumbersome, it’s – unfortunately I didn’t think of this earlier, but I thought 853 had a succinct way of indicating that it – what you’re really doing is you are – actually HIPAA itself, HIPAA Security Rule itself has –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

It' says automatic log-off is what it says.

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

I thought it had – okay, maybe I'm mixing my – what I've seen as most understandable is where you remove access to the information on the screen until the user re-authenticates or terminates the session.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Ah, yeah.

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

Because you really want to include that if the original user comes back, they can't just move the mouse, they actually have to re-authenticate to get access back to what they were looking at. So it's either a re-authentication by the original user, a proper authentication by an authorized user. So often times in a clinic the workflow is that one individual brings the patient into the room, takes their blood pressure, enters the information and then locks the screen. A different individual, probably the doctor, authenticates and gets the exact same screen. So you need to be able to support that kind of a workflow where it's either the original user or an authorized user unlocks the screen.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

So, and I don't think it's block access to information, I think it is the application because you still might have information on the screen, but it's just the application they were using. But how – so you would reword it as, automatically block access until they – would you give Julie the – suggest the words.

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

So it's block access to the PHI until the original user re-authenticates or another authorized user authenticates.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, authenticates, okay. And then the second one remains how it is, yeah, that's –

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

The pro – I think we want to make it clear that they'll blank the screen as well, not just have it so that you are logged off, but that you can't see the other data. Sometimes the system will log you off, you can't go to another screen, but it leaves that screen showing with PHI even if the person walks away and does not care to stay logged on. We're already very complicated with the way we word it, but I just wanted to throw that out there.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

That they would what, I didn't hear the last part of what you said.

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

I think that what we have already is getting pretty complicated, but I wanted to throw out there that we did want to be blocking the currently shown screen as well, after the predetermined period of inactivity.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yes –

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

Because sometimes – I’ve seen systems that will log you off, but they leave the screen up so there’s PHI showing, even though you can’t do any – change anything.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Huh, really, well that’s –

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

And that would be bad.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

– log-off part. But I think you’re talking two things, you’re saying block access to the current session or something like that.

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

Well, I think, I think – this is David. I think John’s language covered it; it was block access to PHI.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Uh huh.

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

So that would cover currently displaying or any deeper data. So I think it’s covered, I think the concern is valid, but I think the language covers it.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay.

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

And the – one of – the other reason for my careful wording was you can then do screen – or you can do application-based blocking so that the whole desktop is still available, but the EHR itself is an application on the desktop and just the application is the thing that’s blacked out. Versus – and screen blanking, so the whole workstation is also legitimate, right, so it allows for flexibility.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, yeah. Okay.

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

I think we also need to make sure it covers the use case of a session following, when you – your session migrates with you to another device, but in those cases, you still have to re-authenticate at the next device to access the data. So I think we’ve covered that case as well.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah.

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

But I don’t think we want to re – I don’t think we want to micromanage and say, you have to blank the screen, there are all sorts of ways to do it.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah.

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

Right.

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

We just want to make sure that they're hiding PHI and I think the way that it was worded before, although it sounds in – I think it's probably correct.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, let's – I think we've got that one. Let's go to the next one, the final one and this one – next slide, please. This one is interesting because I looked at the list that Lisa had created for the applicability statements and I realized that, as we were talking, but then I went back and looked again, and that 2014 requirements no longer have any general encryption criterion. The only encryption criterion is number 7, end-user device encryption and I thought well the last one, or not last one, 8 addressed like if you have a TLS channel, it both encrypts and authenticates and – protects, but the criteria don't address the general case where you need encryption.

So I went back and I thought that there were encryption requirements there, so I went back in the 2011 and I discovered that these encryption requirements that are in the 2011 edition, general encryption and encryption when exchanging, which I'll show you in a minute, totally went away in the 2014 edition. So, next slide, please.

So I – Kate Black helped us – explained to us why this was that they felt that independently tested encryption functionality didn't ensure that it was tied to the transport of that information. And they – so they wanted to tie – make sure that all encryption was tied to another functional requirement. And so the only, I think it's in the next – go to the next slide. The only place general encryption, no this is the 2011; these are the requirements from the 2011 edition. The general encryption says encrypt and decrypt electronic health information in accordance with, basically this is FIPS 140-2 NXA and then the encryption when exchanging is the same thing, the FIPS – one of the algorithms that are approved by NIST, which are listed in FIPS 140-2 NXA. So, next slide.

So in the 2014 edition, the only place encryption requirements come into play are in the transport standards, which call for the Direct protocol or XDR/XDM. And the end-user device encryption, which is still in the security requirements, the view, download and transmit, refers to a secure channel. And then there is secure messaging. So those are the – so there are no – there's no coverage about something like if you, Peter brought up the example about a cloud, like if you have a service in the cloud, there's no requirement for any other use of encryption that a product might have to use the algorithms in FIPS 140-2. So, they could use any – anything would be acceptable. So I personally think that that's a problem and I think that they need a criterion that says, if you encrypt data at rest or in transport that the – you must use one of the algorithms that are approved by NIST as specified in FIPS 140-2. Oh, next slide please.

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

So Dixie, I'm not sure I understand what you're trying to fix. I mean we – the carve out that they've done for encryption, like you have walked through, has been very specific because a general rule was being applied inappropriately. So I am very hesitant to agree to just simply bring back a general encryption rule, because it will reopen up the question of just simply using an algorithm does not mean that you're

secure. You have to have appropriate use of the algorithm and you have to have appropriate key management. So, I don't think that we should bring back a general rule. I think –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

No, but –

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

– the people who are using cloud; there is already sufficient guidance in the security rule that has them use risk-based approaches to use the appropriate encryption technologies that is managed by their risk assessment.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

But that is a HIPAA requirement, that's not a certification requirement. And so I can't – I think that, yeah, I totally agree with you that there are lots of – there's the strength of the algorithm but there's also how the encryption is integrated, there's how the key is managed, there are al – the strength – the strength of the key itself. There are all sorts of variables that make for secure encryption, no question about it, but it seems to me that if a product uses encryption, it should be required to use one of the approved algorithms, not just something it DES-1.

That's where I think, I mean, I agree that even adding the general requirement you're just adding the algorithms, you're not adding key management and all the – and secure integration and all the rest, you're not adding any of that. But, you're adding something, you're saying at least the algorithm must be strong enough as Triple DES or AES can't be just anything you come up with. So that's my – that's what I'm trying to fix is if they use encryption it seems like they should be required to – and the biggest thing that I think – the biggest thing I think that would be most likely is TLS, because I think that many products will use TLS for multiple purposes. And right now we have the integrity requirement for TLS in there, but we don't – that's what the integrity requirement says, but we don't have something comparable for encryption.

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

Yes we do, the transports absolutely have encryption, authentication and integrity protection as requirements in all of the existing transports.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

In all of the exist, right, but that's just Direct and XDR/XDM. You might use –

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

So what other transports are there?

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

You might use TLS for other connections; you have connections with even remote services, even – let's say if you're product, well, I said that before. If your product is a software as a service, is there a requirement in there that if your product, if your module under certification is a software as a service product, there's no requirement that the connection to it use one of the algorithms in 140-2, none, because you're not going to connect with Direct, you're going to connect probably using a RESTful interface and there's nothing there that says it has to be – it has to use one of the approved algorithms.

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

What are the chances if you use out of the box TLS that it doesn't default to one of the approved algorithms, is that a very likely chance these days?

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yes.

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

No, it's not, not unlik – I mean it's almost a sure thing.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

It's going to go with Triple DES, not DES-1 or 2.

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

No, not true, it'll go with AES, it'll go with SHA1 and it'll use RSA for authentication.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

And SHA2 is what's in NXA.

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

Yeah, and we can get into the SHA2 discussion.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

And you know they update the NXA as well. I don't know, there is no such thing as out of the box TLS, I don't think, I think people just im –

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

Well, this –

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

Can I – this discussion. It may not be our role, this may be a policy decision not a standards decision, but really, this is more standards than anything. I and we at DrFirst, and I'm wearing my DrFirst hat here also, have a humongous problem with the requirements that use Direct and only Direct for this. There are a lot of reasons why Direct is not the right choice here, it may have to do with the discoverability, with the fact that it's so expensive that a lot of centers are using one Direct address and having multiple people share it, which defeats all of the purpose of Direct, except for keeping it secure in transit. It's not accessible and it's just not a really good solution, there are a lot of other solutions out there that are not as – with the traction nationally. But I don't know if this is the place to put this or not, it probably is not, but we need to start working on coming up with allowing other solutions other than Direct because Direct is really is bad. I have prepared a document with one of my co-workers in DrFirst, I'd be happy to share with our group about why there's a need for alternatives to Direct that I'd be happy to share with this workgroup.

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

The problem –

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

I'm more confused with you somehow perceive that you can only use Direct.

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

Yeah, and this isn't the right –

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

You are not in any way constrained to only use Direct. You must at least have certified with Direct, but it's not the only – you are not forbidden for using other things.

**M**

And each user's required to use Direct.

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

– other things all the time.

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

And the problem isn't with Direct, the problem is the way Direct's being implemented, there's nothing wrong with Direct, it can be done perfectly free, it's just the way these trust wars are being played out, it just makes it expensive and cumbersome, but that'll get fixed. But that's way off subject for this topic.

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

Okay, I just thought I'd bring it up since every time I see Direct I get smoke coming out of my ears.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, no, it's the trust issue – they seem to be well understood, just I think, I hope, well, I know ONCs also trying to address them.

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

They're getting resolved, they will.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

But I, first of all, this – it's important for us to always remind ourselves that the certification criteria doesn't say anything about what you actually use, HIPAA has more to do with what you actually do. But certification criteria have to do with what you get certified to do. So, I'm hearing from you guys that you think its fine just that the encryption are embedded in other places and it's adequately covered.

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

This is John Moehrke; I think it is adequately covered. I was kind of pushing back on you to see if you had a potentially better way to deal with it. Because the original way to deal with it produced really bad results. The original way was to say, your EHR has to have some kind of encryption somewhere and it was then implemented as nothing but encryption with no key management and it was absolutely far worse than have said nothing. So that's why the current rule has encryption in the context of specific transports in specific ways, i.e. the Direct Project has it's specific standards for which it uses encryption, XDR uses TLS with mutual authentication and dah, dah, dah. And when you can get specific, it is very testable –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

I see what you're saying.

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

To just simply leave a generic, when encryption is used, it shall be a FIPS encryption, I don't have a problem with the concept, I have a problem with the execution of it.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well the general encryption, looking back at it, yeah, it just says, encrypt and decrypt, it does, it says, to be certified you have to encrypt and decrypt.

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

Right.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

I agree I can see how that would be problematic. But you think it also would be problematic to say that if encryption is used in your module that the algorithms must be those – selected from those in 140-2.

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

I don't see how you would make that a certification criteria.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Um hmm. Okay.

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

I certainly don't have a problem with it as guidance, I certainly spout those words myself quite often. The fact is, I actually get a little bit more explicit about shall not use anything but, but it has to be in the context of the specific use case and the way in which it's used, which includes the environment around the encryption, including the enveloping and management of keys, management of ephemeral keys, creation of good randomness. There are a huge number of things that are needed –

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Those aren't –

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

– and that's why when you put it in the context of something like Direct or XDR, it's very clear, even end-user device I'm not, I don't particularly like the way we did that, but it's at least consumable.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, that's what I was going to ask you about because it's – yeah, that's exactly what the end-user device says.

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

Yeah, I've made plenty of comments about the end-user device encryption doesn't tell you how to manage the keys, and therefore you could completely do the end-user device encryption with a fixed key for all devices, and that would be very useless.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Well, we could suggest a criterion that addresses the protection of the keys, because we don't have – none of them have that.

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

But again, what do you say? Usually the protection of keys is platform specific, JAVA has its way of protecting keys, Windows has its way of protecting keys, and IOS has its way of protecting keys.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Yeah, the testing would be, yeah. Yup. Okay then, we'll say nothing about that one, sounds like. Okay.

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

Sounds good.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, it's – unless you have other points you want to bring up, I think those are – that handles all of our topics for today. Other? Okay, Michelle, I think we're ready for public comment.

**Public Comment**

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

Okay, thanks, Dixie. Operator, can you please open the lines?

**Caitlin Collins – Project Coordinator – Altarum Institute**

If you are listening via your computer speakers you may dial 1-877-705-2976 and press \*1 to be placed in the comment queue. If you are on the phone and would like to make a public comment please press \*1 at this time. We do not have any comment at this time.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Okay, thank you all for dialing in and I hope you all have a good holiday weekend.

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

Thanks, you too, Dixie. Bye everyone.

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

Bye everybody.

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

You, too.

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

Thanks, Dixie. Have a great weekend everyone.

**Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates**

Bye, bye.

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

Bye, bye.