



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
April 8, 2015**

Presentation

Operator

All lines are bridged with the public.

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

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Standards Committee's Transport & Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please also 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 & Associates

I'm here.

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

Hey, Dixie. Lisa Gallagher?

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

Here.

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

Hey, Lisa. Aaron Miri? Boban Jose? Brian Freedman?

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

Here.

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

Hi, Brian. Jason Taule?

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

I'm here; thank you.

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

Hi, Jason. Jeff Brandt? John Hummel?

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

I'm here.

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

Hi, John. Lee Jones? Peter Kaufman? Scott Rea? Sharon Terry? Steven Lane?

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

Present.

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

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

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

I'm here.

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

Hey, Jeremy. Any other ONC staff members on the line?

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Yeah, Mike Lipinski.

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

Oh, I'm sorry Mike, I knew you were on; sorry about that. And with that, I'll turn it over to Dixie and Lisa.

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

Okay, this is Dixie Baker. I'd like to thank all of you for attending or dialing into today's call. Most of today's call will be devoted to kicking off our review of the notice of proposed rulemaking that contains the 2015 certification standards and criteria. But we did want to...and we'll start with an introduction of the NPRM that's being given to us today by Michael Lipinski; so thank you very much, Michael, for joining us today. So that's the main objective of the meeting.

We did want to mention that our recommendations regarding the roadmap were sent to you, the final recommendations were sent to you with the meeting materials and we wanted to thank you all for your participation and all your hard work in getting these roadmap recommendations in place where we're

proud of what we have and we really appreciate your participation. Lisa, would you like to add anything before we go ahead with the introduction from ONC?

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

No thank you, Dixie.

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

Okay; with that, why don't we proceed with our introduction to the NPRM from the ONC.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Good afternoon everyone; this is Mike Lipinski with ONC. For those of you who were on...listened in to the Policy Committee call...the Health IT Policy Committee call yesterday, we gave our first overview of the rule, the 2015 edition proposed rule jointly with CMS's presentation on the EHR Incentive Program, Stage 3 proposed rule. So today I'm going to walk you through a similar presentation, but focusing on some other aspects of the rule than a generalized overview. Okay, we can move to the next slide.

So just...we want to level set on the framework of the rule. So, in the past with like the 2011 edition, the 2014 edition, the criteria were all focused on the EHR Incentives Program and pretty much all criteria one way or another associated with the certification program...excuse me, the EHR Incentive Program, I think maybe just accounting of disclosures was not. And...but what we're proposing now is, if you've followed some of our rulemaking last year, we did a rulemaking and we had extensive proposals and this is some...we received a lot of feedback on that rulemaking and prior feedback and FACA feedback that we got from the Health IT Policy Committee to make a proposal of how our programs more...to make it more accessible to beyond...to other types of health IT and beyond the EHR Incentive Program.

So one quick thing is, we're calling the EHR module now a Health IT module; it doesn't change the definition, the definition of an EHR module before was very expansive, it was like any product or service that could just meet one certification criteria. So we're just changing the name to give more proper attribution to products that have been certified already, like a HISP or something that maybe certified in the future under our program to current or proposed criteria.

I also want to mention...I think worth mentioning here, we, in our last rulemaking last year, we did away with the complete EHR certification for any future editions, so that starts with this proposed edition, the 2015 edition. So, whatever is finalized here, the only thing that could be certified would be Health IT module. And, as I mentioned, by making it more open, accessible, we think we can have requirements as well as criteria available that would support other settings, such as behavioral health or long-term and post-acute care. So moving on to the next slide.

A couple more specifics of how we're moving away from the EHR Incentive Program with our proposals here; so before we...our program included policy essentially for the EHR Incentive Program and to give you an example, the biggest one was the CEHRT definition. ONC was defining the CEHRT definition, but really that CEHRT definition is required for the EHR Incen...to participate in the EHR Incentive Program and was essentially designed to meet the policies of the EHR Incentive Program. So what we've done now is that's in...is solely within the purview of the EHR Incentive Program defining the Certified EHR Technology definition; so that's one thing we've done.

The second thing is, if you're familiar with how certification works now, there are what were called...we call them meaningful use measurement criterion requirements. So a Health IT module coming in for certification that has capabilities that would support a meaningful use percentage based measure would have to get certified to these criteria and these criteria are such things as recording the numerator or more expansively being able to record the numerator, denominator and calculate the percentage and produce a report. So that is no longer a requirement for anything that got certified; however, to make clear, it's still within the CEHRT definition.

So if you're going to...if you're a developer and you want to support a provider participating in the EHR Incentive Program, you're still going to need those capabilities to meet the CEHRT definition. But if you're not supporting somebody participating in that program, you don't have to get certified to that, based on our proposal.

And the other thing that we haven't done or aren't doing right now is specifying like we did before in the base EHR definition a number of clinical quality measures that you would have to be certified to, based on the clinical quality measures that CMS had proposed. The whole CQM policies and reporting requirements are going to be in the payment rules, which we talk about in our proposed rule and CMS talks about in their EHR Incentive Program, Stage 3 proposed rule. So what this does, like I said, is makes it more...our program more agnostic, more open to other types of health IT, other settings and you see here a list. So it makes sensibility not just to support the EHR Incentive Program, but again, other settings. And so, moving on to the next slide, I think we have some examples.

So just some examples that are already ongoing with the certification program. So obviously for EHR donations under the Stark Law and the anti-kickback statute, they...you have to be donating certified EHR technology under one of those exceptions and safe harbor. Most recently, last year in the physician fee schedule rule, there was provisions put in for when you provide chronic care management service using certified health IT to do that. Obviously the EHR procurement from the Department of Defense is referencing certified health IT. And then participation in this...it's a measurement program, a quality measurement program the Joint Commission has to be a particular, what they're called I guess an ORYX vendor is they have to be certified to our CQM criteria. So moving on to the next slide.

I'm going to eat up all your time. This is very difficult to see; I believe you were provided a word document indicating this slide as well and I'm just going to quickly go through the slide. So it tries to break down our rule for you from both a developer and provider perspective. We understand that there are I think a total of 67-68 criteria, depending on how you look at it, C3 the reporting CQM criteria is actually reserved right now and will be, like I had mentioned, proposed in the payment rules, the CMS payment rules.

But in any event, it tries to show you like what is required; so, if I bring a module for certification, these are mandatory requirements, so I'm starting on the left column. These are propo...the proposed 2015 edition criteria; your first column is mandatory required certification for a health IT module. Any health IT module brought in has to be certified to those.

The second column, conditional certification; depending on what capabilities you're bringing in for certification, you will also have to be certified to these capabilities. And obviously you guys will be focusing on privacy and security requirements and capabilities within criteria that, depending on what the module has in it, will also have to meet certain privacy and security requirements, but there's also safety-enhanced design. There's a new one in green which is consolidated creation performance, so this

is testing the ability of a product if it's...for instance, it's getting certified as a transition criterion, that it can create...properly create a Consolidated CDA.

So then the next column is all the criteria that support the EHR Incentive Program. So, it doesn't mean your product has to have all these criteria, because it really depends on what the provider is attempting to use; for instance, there are a lot of criteria, there's...I can't remember what the number is, it's either 7 or 8 criteria that support public health reporting, And obviously you wouldn't need all those if you were an individual provider, because you, I believe it's like you're an EP, I think it's only 3 of 7 that you would report on.

And then the last column are the criteria that are unassociated, so to speak, with the EHR Incentive Program. So...which essentially means it's not being referenced as a capability needed to attempt to achieve Meaningful Use under the Stage 3 proposed rule. But the criteria highlighted in blue are criteria that were previously adopted in the 2014 edition support the EHR Incentive Program. The ones in the green are totally new and really there are only about 8 because what we've done there is we've split out some of the capabilities like send and receive for data segmentation for privacy, similarly for decision support, Health eDecision and also, I believe, for provider directory we split out the query response and...query, which you can't really read at the bottom there.

So, just another way of looking at all the criteria that are in the proposed rule, trying to give you a framework of how a developer and/or provider could approach certification to the 2015 edition. And then moving on to the next slide...

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

Michael, could I ask a question? Do you mind if we...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Sure.

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

...ask a question?

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Oh, any...I mean, yes, I'm here to help you guys out, so sure.

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

One of the questions I had about the last chart is that the...all of the security requirements except for accounting for disclosure...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Right.

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

...were required for Meaningful Use 1 and 2, because in 1 they were required for every EHR certified mod...certified product and for Meaningful Use 2 they were part of the base EHR definition.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Right.

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

So I was wondering why they weren't, you know, what's different about them that they aren't in blue in this picture, I don't...I didn't quite understand that.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Oh, so the light blue, I think that was probably a clarification when I was talking with Steve about this. We were only highlighting that column...you're completely correct that there are actually a lot of criteria in those other columns, for instance the middle column and/or the privacy...

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

Um hmm.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

...and security, there were versions of them previously adopted and as to the particular ones you were mentioning, the privacy and security, a lot of what we proposed for the 2015 edition are unchanged compared to the 2014 edition. The reason why we didn't highlight there, we...the purpose of I think this slide deck was really to show of all this new criteria that we're proposing, optional available criteria, trying to level set as to how much of it is actually new and how much of it is criteria that was previously proposed in another edition.

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

I see.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

So that's the, yeah, so you are correct and I know that could possibly cause a little confusion, but we were just trying to focus on that last column to show folks that...criteria.

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

I see. Okay, okay, yeah, that's good. Thank you.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Okay, moving on to the next slide. All right, so here's the new base EHR definition, this will be for the 2015 edition certification. You guys are going to get into...so there's 2 points raised here; the red is new criteria and then if you can see up top, I've noted that the privacy and security criteria capabilities have been removed and actually are part of the certification process. And in some respects this is truer, there are various reasons, obviously, we have in the rule for why we did this, but before...for you guys who are familiar...if you're not familiar with the base EHR definition, it originates with a qualified EHR definition which is a statutory definition in the HITECH Act and all those capabilities that are listed on the left hand are capabilities specified in HITECH that they believe all providers should have in their EHR.

And so then we aligned criteria with that and we tried to scope it based on policy and then also narrow to the instructions of the HITECH Act. And the HITECH Act never referenced privacy and security capabilities as part of the base EHR definition. So...and I guess in that respect our proposal in this edition is more, I guess, consistent with that approach. So...

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

Michael...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Sure.

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

...this is Lisa Gallagher. I didn't look ahead but I'm hoping that you'll provide a little more detail on what a conditional requirement is...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Right.

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

...and the rationale for moving the privacy and security requirements there.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Sure.

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

Okay.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Let's...I think actually Dixie is going to probably focus a little bit on that, but I...I mean I can talk briefly to it.

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

Yeah, I would like to hear from ONC just the thought process and the background on that.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Yeah, I think that's pretty...

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

Yeah and I am...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Go ahead, Dixie.

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

...I wasn't going to talk about that, I was kind of depending on you to cover that as well.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Okay, yeah, I mean I can...I mean it's pretty straightforward, I mean I'm just going to tell you what we said in the rule on that because that is our reason. So, moving on to the next slide, because I really don't want to eat up too much of your time, because I know you have a lot to cover. So this kind of just shows you how you would build, if you were trying to meet...if you were a provider trying to meet the EHR Incentive Program or if you were a developer trying to support somebody participating in the EHR Incentive Program.

So, you have to have that base EHR capabilities, that's actually part of the CEHRT definition and ONC still defines a base EHR definition; so that's the little dichotomy between the CEHRT definition and the base EHR definition and what CMS defines and what we define. So we define the base, as I just showed you on the slide before. So that's at the bottom, because I'm talking here primarily about participating in the EHR Incentive Program, so, that's why the base is at the bottom.

Then I...we put on the other stuff that ONC requires, and I guess this is where I could talk a little bit about some of the conditionals. So, like I mentioned in that other slide, there are mandatory requirements for any HIT module getting certified and that's quality management system criteria and a new one that we propose in this edition, the accessibility centered design criteria, which essentially ask a developer to attest...list and attest to what various standards...recognized standards that are out there for accessibility design, all the way down from ISO standards to 508 compliance.

And then it gets into...so there's that blue line that shows you kind of what ONC defines and then the rest is CMS EHR Incentive Program defined. So there's the CEHRT definition, like I mentioned before, they have the meaningful use capabilities that are required to meet it. There there's additional CEHRT definition requirements that all providers must do, no matter what objectives you're trying to achieve, you have to have this...

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

Um hmm.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

...and these are like patient health information capture, which is a criterion we have and that's to support the advanced directives, record...obviously the CQMs and then family health history, we have two criteria that we propose for family health history. One is essentially you know, in accordance with pedigree and the other one is just recording according to SNOMED family health history. And then the

next thing you build on is what objectives you're trying to achieve within the program and then we have criteria that support all those objectives.

As I mentioned, like if you were...objective 8, it's the public health objective so we have a criteria depending on what measure of the public health objective you try to achieve, you would get certi...have to use certified health IT. I want to thank Jeremy, I think he put a slide, and it's something I'm going to add to my main deck now, at the end of this slide deck for reference listing what each objective is under the EHR so that, for instance, I think...what is it, the...I don't know how to call it, but the security...is securing health information is objective 1 so that's like the risk assessment for certified health IT. And he's listed all the names of all the objectives at the end of this slide deck for you. So that's like how you would still support the EHR Incentive Program; if I can go on to the next slide...

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

Michael, this is Lisa again.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Sure.

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

Can you talk a little bit about why privacy and security are not mandatory requirements, why they're conditional requirements? I think I heard you say because they weren't mentioned in the statute, but...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

No, that's not really why. So why I say conditional is because it depends on what else is in your module; so it's conditioned on what's in your module. So just like safety-enhanced design is conditioned on do you have a capability that we've identified as something that could...has a risk of patient harm? So for instance, like CPOE or CDS, then we make sure you get certified to the safety-enhanced design criterion, which is focused on, excuse me, like essential usability, the NIST standard user-centered design.

So for privacy and security, that's what I mean by conditional. So depending on what you bring forward, you have to get certified to what we've identified as we think are the applicable privacy and security capabilities if you brought something forward and that's, I think, what you guys are going to delve into, is what I was trying to reference about Dixie's presentation is like what we've assigned, whether you think that's right or not. So, I guess like public health would a good one.

If you brought something forward with public health capabilities, we said, you also have to get certified to these particular privacy and security capabilities as well. And I think we identified them as D1 through D3, so that's like your authentication, access controls, your auditing abilities, your ability to do audit reports. And then I think it's also end user device encryption, I think off the top of my head is the other one that we require...

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

Okay, so...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Um hmm, go ahead.

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

...the vendor decl...you know, specifies what functionality their module has and based on that...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Right.

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

...you determine what requirements to certify against.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Exa...that's exactly it. So, I don't have that slide deck here for you; there's a slide that will be in the main deck that kind of shows it from a developer's perspective like if I bring something forward with...

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

Clinical...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

...capabilities in clinical, you know, clinical capabilities or care coordination capabilities, here's what else I'll have to get certified to as well.

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

Okay, thanks.

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

I just assumed that that chart that you have in the NPRM...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Um hmm.

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

...and I guess we should go and double check because I just assumed because you explained that you had adopted what this...the security working group had recommended, I assumed that that mapping to A through G was...corresponded to the exact same matrix that we provided to you before; is that not true? Have there been some changes?

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

I think you'll have to look at it closely, I mean...

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

Okay, so we should look at it.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

So I have to be careful what I say right now because I need to be consistent with what we've said in the rule.

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

I un...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

I know we referenced your work in the rule, obviously, and I think you guys are aware of that, too and that included that work you just referenced, Dixie; so we definitely looked at that. I can't say for sure there is a 1:1 consistency there.

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

Okay, so as we respond to that question, we'll make sure that we do validate that. Okay.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Yeah, exactly and that's the point because like we asked for comment on that, we identified what we felt was applicable to every module for every function...functionality that there would be in a module and we're asking for comment if we've got that right or not. And that's one of the big things you'll talk about is like we don't give the option and we're asking for comments for that, that you can argue that it's inapplicable or infeasible anymore. It's either the interface approach, you document you have that, or you document that you're...or you get certified to these criteria.

So that's, you know, it's a one or two approach; you know, there's no out approach that...and we think that takes away unnecessary discretion between ONC ACBs and so forth. So, we think it's a more clear approach, and I think that's the point, I guess I'll talk to that real quickly on why. So we think this is a clearer certification approach, a developer now knows what they need to get certified to, you know, what...based on what they bring, it's pretty straightforward. We think it's the right capabilities that they should have based on our proposals, obviously, and it's no longer on the provider to piece it together to make sure that they have the right approach...you know, the right capabilities to meet the base EHR definition...so, it takes...it puts it more on the developer, where it should be.

But also makes it clearer to the developer so there's no more of like that concern that they had I guess the first go around with the 2011 edition about that this is burdensome, it wasn't clear, if I was going to have to do this, I had to try to document or explain why this wasn't applicable and so forth. So...and that's about everything we've said in the rule about it, too. So...

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

Um hmm. Yeah.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

...just kind of summarizing that for you right now. Does that help you Lisa?

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

And Mike, I just want to tell you that what...your part of the presentation today is really, really important to us, so, I hope you don't feel too rushed and I don't want our members to feel like they can't ask questions because we might go beyond. This is really important and we appreciate you giving us the time and I would encourage members to ask their questions.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Okay then. I mean I know I saw there was only 20 minutes on there and I know I probably have gone past that now, so...

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

Don't worry...

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

Hey Dixie, this is Aaron Miri and I just want to say, Michael, as a CIO, this is very helpful for me as I'm reading through this and hearing you, so I want to echo what she's saying; it's making a lot of sense for me, again as a hospital CIO.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Okay. So, I think what we have up now, and again yeah, as Dixie said, I'm open to questions, I just didn't want to screw up your whole schedule.

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

Yeah, don't worry about it.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

So, I'm here to answer questions if you have any. So this shows you like...so, this slide here is like, okay now I'm not...I'm a developer and I've got providers in the behavioral health setting or long-term post-acute care, not going to qualify, they're "ineligibles" for the EHR Incentive Program, but I still want to get certified. And so this shows you how that would work.

Like so I'm bringing something in and I'm bringing it in to get certified to the, I don't know, the care plan or the transitions of care. Well to do that, I'm still going to have to do these things below the blue line and that's QMS, accessibility centered design, and this is all assuming they were finalized, right, this is all proposals right now. But I would also have to do the privacy and security, right, which we identified, if you want to get care coordination, that's where all three of those ones above you see, above the blue line, fall in our...what we call care coordination bucket, it's §170.315(b) criter...listing of criteria there. They are identified privacy and security criteria that they would also have to get certified to.

So, and I guess I didn't mention in the prior slide that, a point that Dixie had conveyed and I don't disagree with is that the privacy and security criteria again still...those are not like necessarily particularly associated with the EHR Incentive Program; they do still support a provider's attempt to achieve Meaningful Use under the Certification Program and objective 1. But, you know, as we've always had our disclaimer, they're not a substitute for any type of compliance with the HIPAA Privacy or Security Rule, they're just...they are capabilities to help with compliance in those areas, so. But I did want to mention that point that Dixie had made.

And so that's like the example here; so like there will always be certain certification requirements and if we would backtrack to that slide you guys probably can't read because it's so small, it kind of shows you like, you know, here's the criteria you must get certified to if you're going under the...going through the Certification Program. And then my next slide, I'm not sure what my next slide is...oh, okay.

So I have...so of the common clinical data set, I just wanted to make you guys aware of that, it's a key component of the Certification Program Rule, the 2015 edition. And so under the 2014 edition there's a common MU data set and we're just going to rename that, nothing is changing with 2014 edition certification, but 2015 edition we've added some data to the common clinical data set what we're calling it again. And the reason why we're calling it that again is the more accessible program, no more just focused on MU...meaningful use, so that was part of the change in the name. It's also the common clinical data set is referenced in our interoperability roadmap about...in terms of data that should always move with the patient, data that should be accessible, data that can be...should be available for exchange.

And these are the data ele...categories that we've specified, most of them...almost all of them are structured now so like for instance, we've added immunizations structured...in a structured format, you're looking at CDX there and NDC coding. Vital signs now with a lot of like LOINC coding, I think maybe SNOMED, too. Sex now is required to be coded according to HL7 version 3. Race and ethnicity we have some more granularized coding, PHINVADS as well as obviously the OMB standard. So those are just to show you, because this is...we've also added UDIs in there as well. And next slide.

So this is just, you know, you guys, I'm sure you're familiar with the comment process. We also have the common template available now; it's been finally through all the 508 processes and been corrected due to some errors actually going through the 508 process. We also have a Microsoft Word version of the rule. Any...yeah, so now questions, comments, you want to go back to a slide or anything like that, anything else that you saw in the rule that you had a particular question about?

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

I have a question about...this is Dixie. I have a question about on slide 10, when you briefed slide 10 you mentioned that the original law, the HITECH Act actually defines...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Right.

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

...the base EHR definition. I thought the EHR base definition was introduced in the 2014 edition, that's the first time I ever recall it's being reco...

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Yeah, so you're right about that. So if we can go back to slide 10, I guess. So, yeah, I didn't want to get too much in detail, but if you ask, I will answer. So the HITECH Act references what's called a qualified EHR and it...

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

Um hmm.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

...so back in the 2011 edition we first defined CEHRT as...EHR technology, if you recall, you had to pretty much have everything for setting, so it was either everything for an ambulatory setting or everything for an inpatient setting and you could either do that through a complete EHR or through multiple EHR modules or even a combination of a complete EHR and EHR modules. And if you look at that definition, you'll see a term, it'll say in there qualified EHR that meets the qualified EHR definition and that's...

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

Um hmm.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

...like I said, the definition in HITECH. And what we did in the 2014 edition in that rulemaking was we renamed it a base EHR definition, because we just felt like qualified EHR nobody would know what that means. It was also actually being referenced in other CMS programs meaning something totally different. So, to avoid confusion, and we ha...if you were to go, I could probably find the pages at some point, there's a whole discussion of why we changed the name to base EHR definition. So, you're right we introduced the concept of a base EHR definition, but it's still always consistent with what the HITECH called a "qualified EHR" and particularly capabilities that the qualified EHR must have in it. So...

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

Hmm.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Yeah.

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

Okay, that's useful, thank you.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

So that's where it comes from. Yeah, and if you look in that discussion, go back, we talked about how although privacy and security wasn't mentioned, we thought from a policy perspective it was so important that it should be at least in there and that all providers should have it.

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

Um hmm, um hmm.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

We're just going about a different way to make sure all providers have it now, now we're saying, and which we think obviously if we propose it is a better way, is to have the developers make sure that their product has it and that way the provider knows when they purchase that product they have the right privacy and security capabilities.

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

Yeah, I think so, too. So good, thank you. Are there other questions? Or comments or...? Okay, hearing none, I want to again thank Mike for presenting this to us; it was very, very useful to hear this context before we start our discussion of the specific items that have been assigned to us. So thank you once again, appreciate it.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Great. Okay and I mean, if I could add just one more...two points; one on the privacy and security. So what this does, and I, you know, I gave you a lot of information to digest, but if you just look at like the slide that's up now and the next slide, this means any product that comes through has privacy and security; so it's no longer just like, oh, I'm participating in the EHR Incentive Program, I have to have this criteria, right, because it was in the base EHR definition and that's why you had to have it. Now it's anything that gets certified. So it's not whether that products used for the EHR Incentive Program or for anything else, like in the other examples on the other slide, it's going to have to meet certain privacy and security capabilities. So that's an assurance that the Certification Program is now going to provide.

And then my other point is that, I just want to say you're in good hands with Jeremy, based on my interactions with Jeremy, he knows what he's doing here so, he should be able to help you out. Okay?

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

Yeah. Thank you, thank you so much.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Thank you.

M

Thanks Michael.

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

Thanks Mike.

Michael Lipinski, JD – Senior Policy Analyst – Office of the National Coordinator for Health Information Technology

Thanks. Bye.

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

While we're switching, this is Peter, sorry I got on late. I apologize.

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

I'm glad you could make it, hope you didn't miss too much of that Peter. That was a good introduction.

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

Yeah, all but the last slide.

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

Okay. So now we're moving on to a discussion of the specific items that were assigned to us and so if you go to the slide, please; this is the summary of the assignments; in the middle column lists the assignments that were given to us. In the right-hand column, the ONC staff is specifically pointing to exactly the pages within the NPRM that cover that particular topic.

We've tried to address, right off the bat, the biggest issue was the complete change...dramatic change in how products are certified against the privacy and security criteria. So, we're going to undertake that first followed by three topics that we think will be fairly straightforward. And then in our next meeting on April 21, we'll talk about data segmentation for privacy and the...and data provenance. And finally, on May 6, we'll talk about esMD, electronic submission of medical documentation and auditable events and tamper-resistance. So, next slide.

I wanted to start the discussion by...since most of you, I think all of you except for Lisa and me, are not on the Health Information Technology Standards Committee and although I hope many of you listen in to our calls, I did want to remind everyone that we do have some criteria and metrics that we've developed within the Health Information Technology Standards Committee that define...that are intended to provide guidance on when a technology specification is ready to become a national standard.

And these are...the whole paper documenting the whole methodology is referenced...it's been...it's published in JAMIA, but this diagram depicts there are two primary areas, two axes depicted in the graphic. One is the maturity of a specification itself and the second; the x-axis is the adoptability of that specification. And each of these is further broken down into specific areas like maturity criteria consider the maturity of the specification, the maturity of the underlying technology and market adoption. Whereas adoptability considers how easy it is to implement and deploy, how easy it is to operate with...using that and that criterion considers a lot of factors like dependency between organizations; and finally, intellectual property restrictions.

So as we undertake our discussion of these assignments, I want us to always keep this in mind is, think back to this graphic, if you will, the maturity and adoptability of the specifications that are being recommended to be nationally adopted so that every product has to use this particular specification. Consider whether it is sufficiently mature and whether it is sufficiently easy to adopt to become a national standard because these are the criteria that the Standards Committee will be using. Next slide, please. Are there any questions about that before I go on?

Okay. We've...we're going to try to address...we have 45 minutes left, so we're going to try to address all four of these topics today and we're going to start with the discussion of the model that has been proposed for certifying privacy and security criteria...modules against the privacy and security criteria. So, next slide, please.

I wanted to give you a little history here, because it's extremely relevant. The first edition of the certification criteria, which were published in...which was published in 2011 propos...you know, introduced the whole concept of certifying both complete EHRs and EHR modules and every complete...every product that was submitted for certification as a complete EHR was required to meet all of the privacy and security criteria. And EHR modules were required to meet all privacy and security criteria, unless the developer could demonstrate that the criterion was inapplicable or that it would be technically infeasible to implement.

And so, as you might expect, the EHR module developers, the vendors, complained that the privacy and security criteria often weren't applicable to their products and they felt that going through this documentation of why the privacy and security criteria weren't applicable to their product was costing them money, costing them effort that they thought wasn't justified. To give you an example, there could be a module that did nothing but drug-drug interaction checking, for example. It might not have, you know, doing a time-out when you're doing a drug-drug interaction or requiring an audit; all of the detailed criteria or a back office function perhaps, they don't necessarily need all of the strict privacy and security requirements.

So, as a result of that, the 2014 edition introduced this concept that Mike has just discussed the base EHR definition, which is something that providers need to meet, not that vendors need to meet. So providers...so EHR...base EHR definition was defined as something that a provider must demonstrate that the products that they have selected and implemented are adequate for meeting this whole base EHR definition. So since security was part of that EHR definition, it became incumbent on the provider to demonstrate that if they brought...if they bought modules A, B and C and all of which might have been certified without any privacy and security criteria having been met, the provider might have purchased those thinking they would work together and they would enable them to meet HIPAA and then they might be surprised to find out huh, they don't.

So we...the privacy...what was called the Privacy & Security Workgroup then, now this team here, we felt that this was extremely unfair to providers and also very, very difficult for them to demonstrate...for a provider to demonstrate that the particular set of modules that they had purchased can work together to meet HIPAA. So we thought that this was extremely burdensome to providers and we recommended an alternative, we recommended that every module and every EH...every module must be required to meet all the privacy and security criteria, but we would give them three options. Number 1, they would implement the capability, two, they would document the interfaces that enabled them to get that service from an external service. So they would integrate it wi...this other module and that's where they would get the capability or they would document why it wasn't applicable. Next slide.

But that was...what we recommended still wasn't deemed acceptable and so 2014 release 2, the final rule, actually eliminated the complete EHR certification for all future editions, starting with 2015 edition so that all technology submitted for certification would be assessed as an EHR module. Well this further complicated things because all of a sudden there would be no products out there that necessarily would have been certified against the standard, unless the vendor specifically asked that their product be certified against the privacy and security, it wasn't required of any of them.

So the latest thing that we recommended, we came back and we said, okay, there are some types of modules that may not need the privacy and security functionality and there are others that always, like the clinical module, any clinical module is going to, by definition, need the capability to meet HIPAA. So we came up with a matrix that...Lisa led a team that put together a matrix and said, okay, these are the

types of modules, it's sort of if then statement. If the module does the following things, then it must be certified against all of the privacy and security criteria. If they'd do certain C, D and F, then they must be certified against the first three privacy and security. So she came up...her team came up with this matrix which we said, okay, let's require it of all, you know, depending on what the functionality that the module provides to begin with will determine whether and which privacy and security criteria the module would need to be...to meet and, in addition, if they are required to meet it, they have the three options; implement it, document the interfaces or determine why not. Okay, next slide, please.

Oh, I thought I finished...let me go...go back to the other slide, let me just close it up. What you'll see in the NPRM is that they propose to do just what we recommended except that they provide only two...and they have a matrix in there very similar to what we proposed, but as Mike said, we need to go through and validate that that matrix is correct. But they proposed not to give them the option to...the three options, but to rather give them two options, either technically demonstrate that you have the capability either within that module or by using an external service, or document that the impl...that the service interfaces are implemented for each applicable criteria. There are two...yeah, the one that they...as...the one that they eliminated was you can't document why not, you are required to either implement it within your module or document how you use an external service. So, are there...is that pretty clear?

So we're...this NPRM basically recommends basically what we were recommending, so it's, in my opinion this is way better than where we were before, so it's certainly a step in the right direction. We still need to review it and make sure we all agree that as it's documented in the NPRM, is what we want. So, now the next slide.

This is the matrix I was telling you about. The...one...you see in the left-hand column it says if the module includes capabilities for certification listed under, and these different sections, they're all in §170.315, so...because these are the certification criteria and (a) is clinical criteria, (b) is care coordination, (c) is clinical quality measurement, (e) is patient engagement, (f) is public health, (h) is Direct, the Direct protocol and (i) is the esMD, electronic submission of medical documentation.

So then the column in the middle says that they would take for either approach 1, which is implement exactly what these are or approach 2 is for each of those in approach 1, they would document the interfaces. So one of the things we need to do is to go through that center column and double check that these are the right paragraphs that should be required for the type of modules identified in column 1. Is that clear? Lisa, maybe you could expound on that, since you led the group.

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

Yeah, so what we did was, we looked through all of the requirements and we looked for capabilities that would require access or would facilitate access to clinical patient information. And those were the ones that we felt needed the appropriate security controls associated with them. And that's why you have what's in column 1. And Dixie, I think we should check those to make sure that they match what was on the list, too...

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

Yeah.

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

...meaning, because something could have been left off. But that was our rationale. So really if...the thought process was if the module facilitates access to patient data, then it needs to be certified against security criteria and it either needs to show that it implements those things or that it calls a service that implements them for it or on its behalf. And that's kind of the logic that we suggest. And as Dixie said, it looks like they sort of adopted our approach; we just have to make sure that we're in agreement that they carried over everything that we suggested.

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

Yeah, maybe we could get one or two of you to volunteer to do that mapping and we could give you the original spreadsheet and you could review it against this and check it, rather than everybody having to do that, would there be anybody who would...

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

I was going to say, Dixie, given our timeline, I can't do it because I'll be at conference next week, so, I would be happy to do it, but I just don't think I'll have time enough. If anyone on the team wants to do it that would be great...

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

Dixie...

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

Yeah.

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

It would sort of...help you learn the logic that we went through also.

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

Dixie, this is John Hummel, I'll take that task.

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

Excellent, thank you John; we really appreciate it and we'll put you on the agenda for next time and you can report back to us what you find. We appreciate that.

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

No problem.

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

It's a tedious task, so I don't want everybody to have to do it, but I really appreciate you doing it.

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

Yeah, I'm not going to HIMSS so I have to have something to do.

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

Oh, okay.

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

Thank you, John and I am available for any questions.

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

Thank you.

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

Yeah and we will, we'll make sure that you get the original spreadsheet. Okay, I'll make myself a note. Okay next slide, please. Okay, this is what we've been asked is the proposal is a new approach for privacy and security certification, which is what we've been talking about and the requirement is that a certification body must ensure that the health IT module presented for certification to any of the criteria that fall into each regulatory text "first level paragraph," that's right at the top, category which is the chart we just went over, is certified to one of two approaches, either technically demonstrates or document the external interface. And ONC is asking us for comments on the overall clarity and feasibility of this approach.

Some of you...hopefully most of you have read the description that's in the NPRM, do you see, now that I've gone through and I described how we got there and what we recommended, is the description that's in the NPRM clear what they're asking people to do? And do you think a vendor would be able to look at that chart and figure out what they need to do?

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

This is John Hummel and I think it does because it gives you the two steps and I think they're both clearly articulated so as an end user of the technology, but also as a former vendor, I cou...I would say that would be acceptable.

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

Okay.

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

And so...this is Lisa; I think overall yes, I definitely want...I think we should look at the NPRM at the exact language and make sure we don't have any suggested changes or edits. Since we suggested it, you know, primarily, we can help facilitate its clarity if we see anything that we can suggest.

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

Um hmm.

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

So I will try to do that before our comments are due.

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

Others have comments? I personally thought it was very clear and I think it will be very easy, especially given the chart that we just went over, for any vendor to figure out what they...what the...it's not...it's very succinct, it points to exactly...

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

Yeah.

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

...the paragraph they need to meet.

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

Yeah, the table...the chart definitely helps.

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

Are there other comments?

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

Yeah, this is Aaron Miri, I'm looking at it, it does make sense and I think from a vendor perspective it does make sense. Again I guess, and this is my CIO hat on, my worry is as the various vendors go back through and kind of cost out what it's going to take to bring their systems up to spec, because I think you hit the nail on the head earlier Dixie, regarding what the thought process probably was earlier on versus this, which is very clear; there is going to be some gap, depending on what vendor you're with and how vested and invested you are with them and what it's going to take to shore things up.

So I'm just curious how that's going to translate back to timelines, ETAs and other stuff because I can tell you, a lot of folks are running their EHRs on very antiquated systems that case in point can't be encrypted and things like that without significant investment. So, I could just see some level of concern down the road.

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

Well, what kind of technology can't be encrypted?

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

Well let's assume you're running on an old...

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

I mean, you can have...you add encryption.

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

...right, yeah. I mean, I think anything could be added to, but wh...is it going to be usable at that point? Let's assume you're running on a server that's 7 years old, and suddenly you add encryption on top of that and it brings your spinning disk to a halt, basically, due to slowness. I mean things like that that suddenly make things unusable to the clinician. I could just see some level of investment having to occur with a lot of the hospitals across the country, one way or the other, to make this happen.

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

Um hmm. Yeah, I think the topic of encryption, I think, for too many people call upon oh, the performance impact and in this day in age, there's very little performance impact. Plus, the criterion don't require full disk encryption versus file encryption versus, you know, they give them the option, even if it's old technology, you can always encrypt this file through a crypto module and then put it in

the old technology. So, it's...I don't think that they've made encryption so specific that it should ever exclude anybody actually.

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

Right; and so personally Dixie, I totally agree with you, that's why my first philosophy is, everything encrypted bar none, but, just knowing a lot of my peers across the United States and others, I can see some level of, oh man, I've got to make investment to shore things up.

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

Yeah.

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

I mean, it's a necessary thing that needs to happen because in this day in age, to your point, and I agree with you, it's silly not to do this.

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

Yeah, yeah, but I agree with you too, there will be moaning and gnashing of teeth.

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

Yes, definitely.

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

Dixie, this is John Hummel and I'll just tell you that we recently went live with a certified EMR and because they used an older encryption, it actually forced us to co-opt our roaming desktops...clients and we had to go back to PCs for all of our providers.

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

Really.

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

Yeah.

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

And that, Dixie, hit the nail on the head; that's a very common story on various dimensions, so that's a great live use case.

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

That is a really good use case, actually, yeah. And I'll bet you the vendor never told you about that before you chose it, right?

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

They did not and didn't when they...it through a patch that we were not aware of and it went straight into production and so we were down for the entire day as we rushed around trying to replace...lines with PCs.

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

Uh huh.

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

But the issue is to not dumb our response down because of this, but to make people aware of it and try to have people proactively fix up their systems so they can do it right...

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

Absolutely.

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

...and not be sidelined by it.

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

Yeah, and speaking of...

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

I always worry about us trying to find the lowest common denominator, not us, but people in every industry...

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

Yeah.

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

...trying to find the lowest common denominator because you don't want to get somebody in trouble and ending with a substandard system.

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

Yeah, yeah. Yeah, if we can anticipate some of those, it might be useful to ONC to hear them actually. Yeah. Okay, are there other points that people want to make? We will...when you go and review this, keep your mind open to exactly...to examples like that and the kinds of modules that any of them, any of the requirements might introduce challenges, shall we say. Okay, let's go to the next slide. And we'll go over at the next meeting, Jeremy, put that on our agenda for next time, we'll go over John's mapping of the table to our table.

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

Will do.

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

Thank you. Okay, the second thing...second item that was assigned to us is automatic access time-out. Next slide, please. And actually, this came out of our Privacy & Security Workgroup as well; in fact, it was something that the exercise that we just referenced brought forward is that the old criteria called for a...and in the 2014 edition referenced an automatic log-off and we were saying, well that's not really what you want, if there's...if somebody walks away from their desk for a period of time and they have to be away and its longer than anticipated, 5 minutes instead of 2 minutes, the system shouldn't log them off, but should rather go into the locked screen type of a state.

So we felt that...and it also referenced a session, that if there were a...it should terminate the session and we realized that systems, a lot of systems aren't well web-based systems aren't session oriented at all. So we felt that the reference to session should be eliminated and that they shouldn't reference

automatic log-off, but really shouldn't reference automatic log-off but really should phrase the criterion so that it really addresses the issue of restricting access to protected health information.

So, the proposal in the NPRM is to require a health IT module to automatically stop the user access to health information after a predetermined period of inactivity and require user authentication in order to resume or regain the access that was stopped.

M

That is much clearer and I think really gets to what we're trying to say; that's great.

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

Dixie, is that the wording we suggested?

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

I think it is I know the wording we suggested referred to protected health information, to restrict access to protected health information.

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

Yeah, okay, we should probably check that.

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

You got my vote, too.

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

We should check the...

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

I would suggest...

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

Yeah, and...

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

You know we should because this...if this is a quote, which I suspect it is, it doesn't have protected and I think...

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

Right, I think...

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

...people would have a...

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

...yeah, I noticed that right away and I think we just want to check it with our recommendation.

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

What...

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

The other thing that we might include here, just from a security standpoint is a comment or we could at least consider including a comment about not losing data that had already been entered. I mean, as a clinician, it can be really problematic if you've started to do something in a note and then you're called away suddenly and then if that information gets lost and you're not informed of that somehow, you may think you've done something and it didn't get done and that's a challenge.

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

That's a good point, Steve, the...

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

That is...yeah. That is a good point and if they choose log-off, that could very well happen, if they choose lock screen, it's probably going to come right back to their current state, but yeah, I think that that's a good recommendation.

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

Yeah, and that goes to data integrity, too, I think, I mean...

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

Exactly.

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

Yeah.

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

...it's sort of within our purview, you know.

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

It's also challenging in that the way we've implemented these systems often there are multiple layers that might log-off, you know, there's the EHR application, there's the Citrix, there's the Windows and oft times those can be in conflict if they're not configured appropriately. Again, I don't know if this belongs in our responses here, but it's certainly another challenge that's part of this...getting this set up right.

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

Yeah, that's another problem with the automatic log-off because really a log-off is usually operating system level log-off, but, yeah, it could be at...

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

Well to complement that...

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

...any of those levels, actually.

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

Dixie, this is Jason. To complement that, I totally agree with the changing of the word, but a lot of times you're not just talking about somebody coming back to the same end point where they walked away originally, they may go to another terminal elsewhere in the hospital and they want to pick up the same session that they left off...

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

Absolutely.

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

...which is an entirely different wrinkle on this...

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

Right, they may never go...

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

...which I don't think we have a problem...

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

...back to the endpoint that they were at when they were logged out.

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

...right, so it's not a problem from a security standpoint, but if our requirement is to not lose that data, right, if that's a web interface and we haven't updated that when the person walked away, that data is never going to appear elsewhere in another terminal until it gets saved.

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

Yeah, but talking to that really dictates an architectural design.

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

Right, so from our standpoint, we might want to consider a standard that says, if a user has walked away for x number of minutes, not only do we impose a screen-saver, but we force a current save of the data that's in play.

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

Yeah. Yeah, but I would push back on any requirement that says they can pick up the session on any other place, you know, any other terminal, because it does dictate a design and you don't want to...an architecture actually, not just a design.

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

Well I'm not saying that we're dictat...

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

And I don't think we want to do that.

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

...I'm not saying we're dictating that design, I'm saying that's how it's currently being used. I think the user community is demanding that and we have to anticipate that and talk to the security issues around that use case.

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

Picking up a se...see, that dictates a session-based solution, to be able to pick up exactly where you are is a session-based solution, probably a thin client solution where you have a virtual session on a different machine that you can pick up any place.

M

Right.

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

And I don't think we want to go there and the vendors would definitely push back because there are some PC-based EHRs out there.

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

And it could be a differentiating feature if a vendor's able to offer it that might help them sell it, but not...they don't need to be forced to offer it.

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

Right and some hospitals...this is Aaron Miri; some hospitals can...or healthcare organizations can't even afford to make the investment in a virtual desktop at this time. I mean...

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

That's right.

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

...there are a lot of hospitals out there that are just on the edge right there. So, to the degree of it, I agree with Dixie, let's make this as simple as possible, save and log-off versus anything else.

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

Yes.

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

No, not save and log-off, save and lock.

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

Save and terminate access to protected health information.

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

There you to, right, there you go.

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

Save, hide and lock, but I like the way Dixie worded it.

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

Yup.

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

Okay, so Jeremy could you...well, when we go back to...maybe Lisa, you'll remember which...can dig up which Standards Committee meeting you presented that...we presented both of these recommendations at the same meeting, so maybe you could go and dig up both the chart and how we worded this.

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

(Indiscernible)

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

Yeah, Jeremy, I'll look in my files and tell you the date if I can, okay?

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

Okay, sounds great.

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

And we'll...you can...Jeremy you can have your team make the comparison and point out any differences between our recommended wording and what's in the NPRM.

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

Right.

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

Hey Dixie, can I ask a question? What does the word pre-determined period of inactivity? Is that something that the organizations will have flexibility to determine? Or is that something that eventually will be mandated that is, I don't know, 10 minutes or 5 minutes or whatever? How is that...because I can tell you that in a healthcare setting, it is whatever provider, whatever doc, whatever nurse at any given time will tell you, oh, this should log-off in 30 seconds versus a minute versus 10 minutes or whatever.

And I'm just curious how much flexibility is going to be allowed with that, because I can see that being a point of concern.

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

Yeah, it should be configurable.

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

Okay.

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

It's meant to be con...

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

I thought we even said that, actually when we...pardon?

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

Yeah. I think that's what we meant is it's configurable by the organization, but...and so the module has...provides the capability for the organization to configure it.

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

Yeah,

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

I'm glad to hear that, that makes my life as a CIO a lot easier. Is it may be fruitful for us to add that into this, just to make it very clear because I could see when you come to crunch time as a programmer, and in a previous life I've been a programmer, you will take every shortcut available to make sure you meet the need and if...it's easier for me to hard set a value of 5 minutes versus allow for an independent value to be placed.

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

Yup, that's a really good addition; we'll have that...make sure that that's covered as well. Good point.

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

On that same point, is it just a question of time or might not it also be distance? I know organizations that are deploying proximity controls for access, so either way it should be configurable.

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

Well...

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

Yeah, I don't know that the aspect is required at this point.

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

Yeah, see this criterion is really based on HIPAA and HIPAA says after a period of time, we have to...it has automatic log-off, too, as well but it has a period of time it doesn't have proximity and there...that's a really nice thing to have, but I don't think we want to dictate proximity protection.

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

Yeah...I think that's in the category of things that could be market discriminators. It's clearly...

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

Um hmm.

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

No, I'm sorry, I wasn't suggesting that, I was simply saying that we not force it to be time; either way it should be configurable. If somebody has a distance based or proximity based control that meets the same objective, they shouldn't also have to worry about a time setting.

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

Yeah, I mean, he makes a good point because HIPAA codifies that in terms of time and it probably shouldn't have because it doesn't anticipate the new technology, but...

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

Um hmm.

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

...be that as it may, that's what HIPAA says, I mean, unfortunately or fortunately, right?

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

Yeah.

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

But I hear your point.

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

I think if you...I think if...the thing is, I think if you implemented a system that used proximity detection for this purpose, you would also, in that same system, have a...have it configurable by period of time, you wouldn't have one or the other and so I think the...

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

Well I...

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

...foundation is period of time and if you want...

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

I also...

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

...I yeah.

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

Oh, I'm sorry.

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

I agree with Lisa.

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

I would also say that if you were audited and you had that...implemented, you would probably be compliant anyway. I don't think that we take it by the letter of the law.

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

Yeah, that's true.

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

If you had the proximity...they'd say that's fine.

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

Yeah. If there's a way we could word it that covers both, that would be nice, but I have a feeling, and especially since HIPAA talks about period of time. Of course we don't have time there, could be period of distance...no, I'm...okay. Next slide, please. End user device encryption; next slide, please.

Okay, the NPRM proposes no change to end user device encryption criterion and the required criterion consistent...oh, but they just want to change the FIPS, the...right now the recommendation is end user encryption is FIPS 100-well, it's still 140-2, Appendix A, but I...no maybe it's 140-...

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

Yeah, I think it's the...hey Dixie, this is Jeremy. I think what we're proposing there is the latest version of it...

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

Yeah.

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

...is the only change that's proposed here.

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

But wasn't it...wasn't the old version called...well, probably...wasn't it called Version 140-2 already or was it 140-1.

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

It was, but it wasn't the October 8, 2014 version.

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

Oh, I see.

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

Yeah, they just changed it.

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

I see, so it will still be 140-2.

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

Right, yeah, because that came out after...yeah, after the previous certification rule was already...

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

I see that's what you have on your slide, yeah. So all they're doing is proposing an update to the latest version of FIPS 140-2, Appendix A. And 140-2 Appendix A just lists the encryption and integrity algorithms...encryption algorithms that are deemed acceptable by NIST at any given point in time, like they also have the hash functions back there as well as the encryption algorithm. So 140-2 Appendix A is the standard for both encryption and for the integrity criterion for...one...two. Any comments?

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

So we're not just updating...yeah, we want to make this not just the new version, but whatever the then current version is, right?

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

Yeah, I was going to ask about that because it seems like they could update it tomorrow and you would maybe want it to apply to this set of criteria.

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

Yeah, but they ca...they have to...especially since these are certification criteria, so people are building products today against the requirements, so they can't have a floating requirement. So all of the certification criteria have to be to a specific version, they can't be just the latest version.

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

Yeah, I guess you're right.

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

It's Jason. The way the federal government operates with the systems that have to get an authority to operate, the language is, the then current.

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

That's right.

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

So at whatever point you sit for it and that may be a 1, 2 or 3 year cycle, it's the then current version.

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

That's different. Permission to operate is different from certification of a product.

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

Right, right, I'm simply saying we could...

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

Product certification has got to have it locked it.

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

...we could choose the...right, but we wouldn't necessarily want to have to keep updating our recommendation to point to a different version every time a version comes out.

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

Well yeah, they do, that's exactly what they do. They do that with HL7, they do that with all of the vocabulary, every one...every time SNOMED changes a single term, concept within SNOMED, that concept has a version attached to it and any kind of certification criteria have to specifically cite the version because you can't have somebody coming in with a product they've been designing over the past 2 years and you say, oh yesterday they changed the version. You know, you have to, in a regulation you have to cite the specific version.

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

Well as a consumer, that wouldn't leave me with a lot of comfort, especially if the reason is somebody updated a version was to address a major deficiency. HIPAA still requires that we, as the consumer, do that evaluation. Well if there were a deficiency and they updated it, then they might put through a special change notice or something.

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

Right, right...

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

But you can't have a...you can't have optionality in certification criteria like that, you know, they...I've certainly never seen in a certification criteria, whatever's enforced, but I have seen it in DoD systems that are being approved for operation.

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

Okay, that makes sense.

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

And oh, by the way, the...as far as encryption is concerned, the October 8 edition for encryption standards is no different from the existing. So, I'm not sure why they updated it, but...because it still calls for AES or triple DES. Or I don't know, Jeremy, you're the expert on encryption, do you know of any other...any specific substantive changes where the encryption algorithms in that?

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

I'm not aware of any substantive changes.

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

Yeah, but I guess they're just trying to keep up. So, next slide.

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

I'm sorry Dixie, this is Aaron Miri. Let me ask one more question; is there any need for us, I'm just playing devil's advocate, need to reference anything around cryptographic algorithms, key lengths; I know that NIST has a publication 800-131 A that kind of tells you what the recommendation is for different key lengths. Is that worthy of us putting it in there or is simply referencing this one standard enough?

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

Well, this standard references algorithms, it says, these are the algorithms you need. But it doesn't say anything in Appendix A at least, about key lengths.

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

Right.

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

But the algorithms themselves, I think, have minimum requirements on key length.

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

They do, I'm just asking in terms of us being specific, if it's worth us calling out.

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

I don't know; Jeremy, what do you think? I know you're ONC, you can't express your...no, as an encryption expert, what are you thinking?

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

You have to buy me a drink first. But yeah, we certainly welcome any comments on this particular part, if there are things that the workgroup members believe that are not encapsulated with Appendix A of FIPS 140-2 or if there are other NIST standards that we should be citing here, we certainly welcome that feedback.

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

And Dixie let me give you kind of a real world example why I asked this. So, I'm not going to name any vendors names at all, but there's one very prominent vendor who, as they deploy their EHR in your health system, they also give you a model of what it's supposed to look like and all the user name and passwords for that are like admin admin, right? And it's just the way they deployed at multiple health systems.

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

Uh huh.

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

Well given that, I now have basically a back door into things; if I knew that, I knew what servers to hit and what to log into and things like that. So to the degree of it forcing certain criteria, either explicit or applied or referenced, I feel is worthwhile because it was...I literally saw a brute force attack trying to occur on that model system at a previous...in a previous life. So, just feedback of what's going on.

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

Well, and that's not really key length, that's the system should be deployed so that that password can be used once and then is forced to be changed.

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

I absolutely agree and I took it to the nth degree, right, naturally, so...but right, you're absolutely right.

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

But if that's, you know, that could be a criterion, key length could be a criterion, too, I don't mean to say it's one or the other. Do we want to talk about those, they're certainly both important.

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

Yeah, complexity is really what I would go towards, but yes.

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

Oh yeah, they talk about entropy, yeah. Entropy and the keys; they don't talk about entropy and having to change the pass...admin password. Hmm, so do we want to talk about key complexity and deployed with...hmm, passwords that only work once and then you have to change them? Is that too specific; I don't know. It certainly is important, no question about that, especially admin passwords.

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

I just think we have enough...

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

We can make that recommend...

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

I just think we have an opportunity to influence the course of how this goes in the future and I just think the sooner we start introducing additional layers, the better, I think, in the long run. So, to the degree of it, it might be additional burden overhead and I can just hear the sighs from programmers, but I feel, especially given sort of peace of mind and given the patient data now and the value of it, it's worth it.

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

Can you provide us some words to consider for both of those, key length and changing...

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

Happy to.

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

...okay, great, great, thank you. Okay, and last, I think...oh, next slide is the data integrity. I think this is a...next slide. So we're coming up on the end, but this is our last one, I think we have a chance here. The NPRM proposes no change to the criterion, but proposes that testing against a criterion focus on the receipt of a summary record. It was...you know, I had heard about this issue before, it's too hard to demonstrate that you've run the hash function on the data where the hash function is applied. Where you can really test it is at the other end where the data are received and you can prove there that the hash function...what hash function was used. So they're just saying, make it clear that it's tested at the en...upon receipt and not upon sending; that makes sense to me.

But they also brought up the issue of SHA-1, SHA-2; this was...we addressed...the Privacy & Security Workgroup went round and round about this several years back. SHA-2 was, even then, was the current recommendation but so many vendors and current products were still using the secure hash algorithm, SHA-1 that they said well we really can't impose SHA-2 on vendors at this point. Is it time to change that? And they've pointed out in the NPRM that Microsoft and Google plan to move to SHA-2 no later than January 2017. So, we're still a little ways away, but should we, if they're asking, if and when the NPRM should set the baseline for certification integrity to SHA-2? When should that happen?

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

This is Aaron, I say sooner rather than later.

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

I would agree; this is John Hummel.

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

I don't understand the when part of it...this is Lisa. I mean, they're saying, should we impose this for the 2015 edition or not, I don't know about the when.

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

Yeah.

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

What is the when...

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

Well, or we might say 2017, let's say.

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

So...one reason...

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

No, I...sooner.

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

It wouldn't be the 2015 edition, then, I guess; that's what I'm saying.

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

Right, right, they're saying, should it be the 2015 edition or later.

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

Or later, okay. Just a poorly formulated question.

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

Yeah, you're right.

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

Yeah, this is...

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

I'd say sooner.

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

So I'm hea...

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

Yeah, this is Jeremy. For clarity, the...what we're asking, if not now, when would be a proposed timeframe?

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

Right, that's exactly right. Yup. Yeah, that was Jeremy, he's our official word. So I'm hearing...

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

I think...

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

...is 2015.

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

Yeah.

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

Yes, I'm hearing that, too. Okay. Anybody object?

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

Well, and I mean, so let's give some meat to why now, to change certificates, to change all those things, to get that it's going to take some process, so sooner rather than later so that way we're not left to play catch-up, it would help getting ahead of the curve as folks change.

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

Um hmm. And the Direct protocol requires that both SHA-1 and SHA-256, which is SHA-2, one flavor of SHA-2, be supported. So any Direct exchanges would be able to move to SHA-2, they'd already be there. So basically Direct has already moved to SHA-2 if every place already has to support both.

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

Good point.

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

Yup, that's a done deal.

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

Okay. All right, that's our recommendations, so, are there other comments before we move on to public comment. Okay, thank you all for dialing in today and this has been a great conversation, we're well on our way, this is the...the NPRM has lots...it's long, but it has a lot in it and I hope you guys are taking the time to look at it, especially the security pieces, especially since ONC is helping us, directs us exactly to the right pages. So, we appreciate that.

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

Thank you.

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

(Indiscernible)

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

Are you ready to open the lines for public comment?

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

I believe somebody was just saying something.

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

I just said thank you.

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

They said thank you.

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

Yeah, this is Lisa, I was just thanking everyone for their...

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

I was about to say goodbye until I heard about the public comments.

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

Don't forget public comment. Lonnie, can you open the lines?

Public Comments

Lonnie Moore – Meetings Coordinator – Altarum Institute

Yes, 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 telephone and would like to make a public comment, please press *1 at this time.

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

I don't hear any public comments.

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

Yeah, we need to wait a little bit longer than we have been, so...because there was a lot of public written comment that we will have to share, but there is no public comment people calling in, so, we're all set. Thank you everybody.

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

All right.

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

Thanks everybody.

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

Thank you. Have a good evening. Bye, bye.