

**HIT Standards Committee
Privacy and Security Workgroup
Transcript
April 11, 2014**

Presentation

Operator

All lines bridged with the public.

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

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

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

I'm here.

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

Hi Dixie. Lisa Gallagher?

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

Here.

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

Hi Lisa. Chad Hirsch? Dave McCallie?

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

Here.

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

Ed Larsen? Hi Dave. Ed Larsen? John Blair? John Moehrke? Leslie Kelly Hall? Mike Davis? Peter Kaufman?

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

Here.

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

Hi Peter. Sharon Terry? Tonya Dorsey? Walter Suarez?

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

Yes, I'm here.

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

Hi Walter. Is Julie Chua on from ONC?

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

Yes, I'm here, hello.

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

And Kate Black from ONC?

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

I'm here.

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

Hi Kate. And with that I'll turn it back to you Dixie and Lisa.

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

Yeah, I should tell you that, Michelle that Tonya Dorsey, when I sent out a note to her this week it bounced back and so I asked Anne Castro and Tonya has left Blue Cross Blue Shield South Carolina. So, Anne Castro is going to get us someone else to take her place. So, I'm not surprised she's not here today. But thank the rest of you for coming.

We – I know I also invited the Implementation Workgroup to send representatives and they talked about sending a couple, is anybody else on the line from the Implementation Workgroup maybe? I know Travis was one of the people they were going to ask David?

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

Yeah, I haven't seen him today, I don't know.

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

Okay, all right.

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

It would be great if he'd join us, but –

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

I know, I know, but we'll be briefing or I'll be sending a summary of this discussion to the Implementation Workgroup and, you know, we may be having further conversations with them because we do need to coordinate it with the Implementation Workgroup.

The agenda for today, the primary focus is our one last item on this NPRM review which is the certification of EHR modules against – well, actually its certification of EHR technology since everything is modules at this point against the privacy and security standards.

But I did want to make sure we have – we have a couple of balls in the air and I wanted to make sure people knew where we were on things. The Standards Committee will meet the week after next and we have two slots on the agenda, one is to brief them on the NSTIC Hearing and Walter and I will be presenting that briefing and the other is to present our responses to the NPRM. Julie's MITRE team is in the process of putting that into – finalizing our responses so far and we'll add the response for today and distribute it for review and perhaps if needed we'll have an additional meeting.

The NSTIC slides, Walter and Lisa, and I have reviewed them and I think I sent them to everybody for comment and asked you, I'm pretty sure I did, if you have any comment about those slides or any suggestions please give – you know, send them to me and unless we have, you know, some controversy or need for discussion we will not have a meeting to discuss those we'll just be presenting them to the standards group.

So, do please take the time to look at them and make sure in particular that we've captured the points that you think are most important for us to make with the Standards Committee. Okay, with that Lisa do you want to add anything?

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

Oh, no, Dixie, I think you covered everything. I think, you know, this presentation that we're about to look at –

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

We can't – you're breaking up very badly.

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

Okay, well, I'll just turn it back to –

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

Okay, can you hear us okay?

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

I can.

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

Okay, good, good. Okay, with that let's just start through our slide deck. I think somebody else is controlling them right? Okay, I wanted to just – this isn't the beginning of the slide deck? Yeah, yeah, thank you. I wanted to start by just – I know there have been a lot of machinations within EHR technology certification and I wanted to make sure that everybody knows that full context.

In 2011, there's two editions out 2011 and 2014. The 2011 edition requires that all – defines, that's the one that first defines complete EHRs, says we're going to certify complete EHRs and we're going to certify EHR modules, and it says every module and every EHR, every complete EHR must comply with all of the privacy and security certification criteria.

And as a result of that some of the module vendors complained that the privacy and security criteria often weren't applicable to their products, they would be, you know, maybe even a back end module that didn't have users or for some other reason. So, they ended up getting waivers, giving a lot of people waivers.

So, when it came out in 2014 they defined a whole new way to certify technology and in fact to even, you know, demonstrate that you're using technology meaningfully, they came up with this idea of the certified EHR technology and the base EHR and the complete EHR they still had to see – the complete EHR and the EHR modules but they said, you know, the privacy and security requirements are the responsibility of the base capability and that's not something you certify that's a part of the complete EHR or the complete EHR technology, certified EHR technology.

They said, at that point, that the EHR modules are not required to meet any of the privacy and security criteria and this group said that, you know, this really would leave – since providers could put together, could come up with certified EHR technology by putting together a group of modules it's quite possible that they could come up with a set of modules that wouldn't allow them to meet the HIPAA requirements. We did –

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

Dixie, can I just interrupt you for a second, this is Kate from ONC?

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

Yes.

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

I just wanted to clarify one point about the base EHR definition in our 2014 rule, the way it's structured through our certification program each and every provider that was going through Meaningful Use would have to meet the base EHR definition.

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

Right, but we're talking about what vendors would have to meet. The providers, yeah, would have to meet the base EHR definition, but the vendors would not.

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

I wanted to make the point that no provider would receive technology that did not have privacy and security criteria in it.

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

Well, I would argue that they could. They then would not meet the base EHR definition, but –

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

Which they have to do to meet Meaningful Use.

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

Right, so the onus is on the provider to make sure that they have the base EHR technology not on the vendors who produce the technology. So, we did, at that time, say that we certainly understood that it was better – you don't want every single module having a different security solution.

Ideally, you want to have a security solution that, you know, that one module provides and all the others use that service through a standard interface. But, we did not agree that the modules should not have to meet any privacy and security criteria.

And I'll show you that we recommended, and the Standards Committee endorsed, we recommended that individuals be or that vendors that were submitting EHR modules for certification be given three paths that they could choose between to meet any one privacy and security certification criterion and I'll review those with you in a minute.

The current NPRM that we're reviewing has a question that I did distribute with the materials for this meeting, but first of all it proposes to drop certification of complete EHRs entirely so that all EHR technology that is certified will be certified as either a Meaningful Use EHR module or a Non-Meaningful Use EHR module.

And they request feedback on the approaches, on four approaches for certifying EHR modules against the privacy and security criteria for consideration in 2017 and the first is going back to the 2011 approach, the second is the 2014 approach, the third is what we recommended, the Standards Committee recommended and the fourth is to propose a subset against which all the modules would need to be certified. Okay, next slide please.

This is a recommendation that we made in December 2012 and it was endorsed by the Standards Committee and what we recommended was that each EHR module would be required to meet each privacy and security criterion but they would not be required to implement every privacy and security criterion in the technology rather they could either implement it in which case they would demonstrate through their certification testing and documentation that they've actually implemented that functionality or they could demonstrate that they received that functionality, were able to get that functionality from a documented service interface or third they would demonstrate, through documentation, that the criterion was not applicable or was technically infeasible. Okay, next slide.

We also – ONC asked us to recommend a minimum set and actually the Privacy and Security Workgroup started out with a more minimal set than this and the Standards Committee recommended we include literally all of the criteria except the accounting of disclosures which was optional anyway. Next slide.

So, this is – the paths one and three that are in the NPRM are basically the 2011 edition and path two is the new – wait a minute, path two – I think he's talking about – wait a minute – he's actually, I got ahead of myself, he's talking about the – no he's not, no he's not – the path – paths one and two are the 2011 edition and path two is the new one which is what we recommended.

The path one creates a risk of having multiple modules with incompatible security and two and three don't require testing. He's talking about the paths toward – he's not talking about the models he's talking about the paths to be – that the vendor can choose from to be certified.

The NPRM quotes that 70% of 2014 modules that were certified against the 2014 edition were certified to at least one privacy and security criterion and more than 50% of modules have been certified to four or more privacy and security criteria and that this is impressive, you know, this is evidence that they're implementing them anyway. I question whether that's meaningful because to me that means 30% don't but maybe 30% don't need – it doesn't say much to me.

There are two things that we know, we know that – we don't know – we don't know the scope of what capabilities they're going to be putting in any module because a module is anything that meets at least one certification criterion and we don't know the existing operational environment that the module will be ultimately operating in, and as was pointed out before, that's where the certified EHR technology with full base capability needs to be demonstrated. And Steve also noticed that – suggest that we work with the Implementation Workgroup in addressing this, which we are. Next slide, please.

This is – these are the four options that I went over, this is what's in the NPRM and it includes the recommendation we made in 2012 and it seeks comment on these four options, first is 2011, in other words every single module meets every single criterion.

Option two is 2014 a module does not have to meet any privacy and security criteria.

Option three is our recommendation of giving them the three paths, but requiring those, all eight, as the minimum set.

And option four is to adopt a limited applicability approach which is to establish a limited set of functionality that every module would need to meet and notes that it has the same downside because every module would still have to meet it. Next slide, please.

I think, yeah, I distributed – so that, option four where it's still asking for a minimum set and notes that there would still be problems that's what – that motivated me to really, you know, stand back and say, well, you know, maybe it's true, maybe there is a minimum set and I distributed to you the spreadsheet that I did whereby I put all nine privacy and security criteria across the top and down – and in the rows down the side are all of the individual criteria that are not privacy and security.

And as you can see in that the criteria are broken up into, what, how many different areas, seven different functional areas, there is clinical functional area, there is the care coordination functional area, clinical quality, privacy and security, patient engagement, public health and utilization.

So, those are the functional areas, you know, in the criteria and I just took a wild stab, I don't plan to – you know, I don't report that this is quantitative by any means, but just looking at what the criterion was I said, you know, which of these is really applicable and for the most part they all are applicable to the clinical functional area, except amendments, there are a couple criteria that amendments – and the amendments criterion is for a patient amending that's not a physician amending it that's a patient amending it.

And so my informal assessment said, well, you know, yeah, when we think – and I think that this – that the discussion in the Standards Committee was along this line too. I think people were all thinking clinical because in the clinical and care coordination areas yeah most of these are, you know, are needed.

But then when you get into clinical quality and patient engagement, public health and utilization it becomes less clear, well it becomes clear that not all of these are really required in that area because some of them really are for clinical like the amendments, like automatic logoff and emergency access.

So, using that spreadsheet then I concluded that there was a subset that could be applied to all clinical and care coordination criteria but maybe would not be applied to the others and so I identified for discussion these minimum sets for each of those functional areas.

And to me the best fit seemed to be to propose the minimal set for each of these functional areas and then for each minimal set allow the use of the three paths that we recommended before. And David when I sent this out the first time, all of you, the version that Travis saw didn't have that third bullet I forgot to include it that those three paths would still be applicable. So, Next slide, please.

So, this is the proposal that I would like for us to discuss and it's based on one through four are based on the spreadsheet totally, just based – and so, you know, like I say, I don't claim that there is anything quantitative about that it was just my feel for what would be required in each of these environments and that would be that the – for care coordination and that all EHR modules would be certified against authentication, access control, authorization and audit basically, and integrity.

And then if it were care coordination or clinical it would also be certified against automatic logoff, emergency access, end-user device encryption. There should also be amendments in there, oh, if it's certified against one or more clinical it would have amendments and this is the one we've had a question about, EHR, if it's certified against public health and utilization I thought it still might have PHI written to end-user device that's why I put that in there, but it may not, so we can discuss that one as well as the others.

And then for each of those, for each – still with each criterion you could meet it, the vendor could meet it using one of those four approaches. So, I'd like to discuss this. Oh, wait a minute, no, no let me go to the next slide first, I forgot I have – David sent this to John Travis who actually is on the Implementation Workgroup, so, and he said that the proposed minimal set and the partitioning was generally applicable, workable.

He noticed some exceptions in that first file management and reporting kinds of modules would have minimal use for role-based access control, but there is no criterion, there is no criterion that requires role-based and I've quoted the, you know, it just says "establish the type of access to electronic health information a user is permitted" so it doesn't require that anybody implement role-based access control it just requires that they implement access control.

Security could be module, products could be modules themselves and I think that this is – I think he said that's absolutely true, but he didn't see the three options and I think that if you had a security product you could, you know, you could still take one of those paths and say this is what it does, this is how it meets it, this is why it shouldn't meet it, etcetera.

And then certification and multiple modules that all use the same security service is uselessly repetitive. I agree with him. He suggested allowing the vendor to attest to certification of a common capability for the modules that then the other modules use this capability. I think this is what the 3b offers and I think this is actually a very common approach because even when they had complete EHRs a lot of vendors would have their products certified as both a complete EHR and the set of EHR modules.

Well, now if you submitted a set of EHR modules, Cerner is a great example of this actually, and they all used one module that had security that provided security and everybody else used that service well you could have that module certified and then all the others could document their interface with it.

And then the last was his comment about the encryption for end-user devices for public health and utilization and I honestly don't know what the answer to that one is. So, is that the end, let me see, oh, and then the final slide I think, yes, the next slide is I received another e-mail from Steve and just reminding us to think about the implications of how they would be implemented in, you know, in actual certification practice as well as operations and again to involve the Implementation Workgroup.

So, could we go back a couple of slides to the recommendation and I would like to hear everybody's thoughts about this.

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

Dixie, before we talk about it, I found this confusing until I looked at the spreadsheet that you also included in the meeting announcement and that helped me get a sense of what we're talking about here a lot.

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

Okay, this isn't the slide, keep going forward please, still forward please, forward please, forward, forward that one, back, that one, yes, yes. So, how could we convey that same thing to people without the spreadsheet?

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

Maybe some kind of table or something?

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

Oh, yeah.

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

So, Dixie, this is David, I wonder if maybe we don't actually need that spreadsheet, because here's where I'm coming from, it seems like number 5c demonstrate that it's inapplicable could be used for any module regardless of whether we have the spreadsheet or not because if it was in the spreadsheet but it's inapplicable you can still get passed it using 5c and if it's not applicable it's going to be easy to justify, it wouldn't be in the spreadsheet in the first place, it would be easy to justify why it's not applicable.

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

Oh, yeah.

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

I mean, 5c trumps the spreadsheet.

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

Right, right, but it could be used to help them make that justification.

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

Well, it might be, yeah, guidance or something but I think, you know, regardless of what the spreadsheet says if you have 5c in place then a module author could argue that it's inapplicable and would have to convince through the process that it didn't apply.

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

I don't – this is Walter, I don't disagree, I mean, I think the first question is whether the two components of this proposal are appropriate first of all. I mean, because I'm – my argument is there is no issue in my mind with respect to the three paths, we're dealing with two different dimensions here, one is applying certain minimum criteria to certain types of functional capabilities or functional areas more than capabilities –

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

Right.

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

That's one dimension and the other dimension is these three paths. I don't think we probably have an issue with the three paths since we already recommended them. I'm just not sure that the complexity of classifying and categorizing specific security criteria applied to certain types of functional components is very practical or doable; it increases the complexity of this immensely in my mind.

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

Dixie, this is Lisa, is our – based on what Walter is saying is, you know, our other choice then is to not have them certified against privacy and security requirements at all? Is that what Steve was proposing?

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

Yes, I – remember, I'm glad you guys both brought this up. When we went through the – I should – when this Workgroup went through the NPRM remember we came across the module question and we said we're just going to resubmit our recommendation from the last time, you remember that?

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

Yes.

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

And I mentioned this during the Standards meeting, the last Standards meeting which was – it was a virtual meeting and I mentioned our intent, you know, to resubmit the same recommendation and ONC, Steve, in particular, who was giving the presentation at the time, urged us not to and said, you know, that's useless basically, it's useless, we want – that's not acceptable. And so I was honestly trying to come to a compromise.

I would also point out Walter there is already an area, I think it's the Meaningful Use criteria, I'm not – I should go and check this, but in the current NPRM they're already proposing another area of certification that does a very similar thing, it says "if this" and that sort of thing.

I also think that you could do this in a couple of ways to make it easier. You could just, you know, reference the privacy and security criteria in those, you know, in those sets of criteria as well like in clinical care for example you could include criteria that say, implement privacy and security criterion 1 through 9 or whatever, right?

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

Right.

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

So it's referenced and privacy and security then wouldn't be a separate – you know, it would be a certification area that was just referenced by all the others, you know, so if we did it that way –

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

Dixie?

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

It would be a little bit less complex.

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

Yeah.

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

Dixie, this is Lisa, I have a question, does Steve or in the NPRM did they say that – indicate any predisposition to be certifying products that are pure security products and don't contain any EHR functionality. I mean is that something that would be incurred in the new certification program? So, you know, you might get security vendors submitting their products for an EHR certification?

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

Yeah that's not – that's not new that's always been something that they've – there have been modules that are pure security.

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

Okay. And so, all right, thank you.

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

You know, so this is David, the bottom line problem here is there is no definition of what a module is and there is no definition of what standard security APIs are, so it's going to have to be left to judgment and anybody can put a module together to do anything they want, so you're going to have to – somebody is going to have to make a judgment that says "this particular security criteria is or isn't relevant to the thing you put together and called a module."

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

Yeah they actually –

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

And I like the idea that –

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

They actually do include a definition but it's so – it just says the definition of a module is any software that implements at least one of the certification criteria. So, it's almost not defined.

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

Right, I mean, you could have –

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

But you know.

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

You could have a module that does, you know, ePrescribing and public health submission, I mean, you know, anything you want is technically can be made into a module. So, I think the best we can do is to describe, in some way, which security criteria apply to which kinds of functions rather than to modules.

So, if the function requires local storage of PHI then you must demonstrate that it's encrypted at REST. If the function allows clinicians access then you must demonstrate that it allows for emergency access and supports role-based authentication, authorization.

In other words, like I think you were headed to, it's not so much a spreadsheet of high level categories but a specific statement of what capabilities correspond to the appropriate security test.

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

And you could – it like if you look at – if you look at the spreadsheet again you could make like, for example, I'm just making this up of course, under clinical functional area you could have an 18 that says, you know, all of these functions – if you implement any of these functions it must meet all the security criteria except amendments and if your – and then your only "if" would be, you know, if your module accepts, you know, implements or records amendments or –

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

Yeah, I mean, this is David again, you could argue that it's better to specify everybody meets everything with the following exceptions or to do it the other way around inverse to say, this function meets these certifications and whether, you know, inverse or original is better is just a question of what the matrix looks like.

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

I really don't – I really don't think that the functional components here are the relevant part. My sense is it doesn't matter if the function is public health or clinical care or –

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

No I agree.

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

Care coordination I think – because I can argue that in public health there could be instances where authentication is needed –

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

Yes.

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

Or access control is needed. So, I'm trying to decouple the functional elements of clinical or care coordination or public health, or utilization criteria, or any of these other things from the core security requirements or criteria and say, you know, these are the core ones that need to be used and it doesn't matter again if it's a clinical or care coordination, or public health there are going to be some – you know, basically a question is if you need authentication for the purpose of which the module was created then you need to apply authentication to it.

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

Yeah, but Walter –

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

It doesn't matter if the module was public health or not.

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

Walter, this is David, I'm saying the same thing. I think it's a function of whether it applies to the – the question is whether it applies to the function not to some grouping of things around use case. So, if there is PHI then you've got to have encryption at REST period regardless of whether it's for public health or not but if there is no PHI then you don't need encryption at REST, right? I mean, that's the –

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

Yeah, exactly.

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

I think I'm saying the same thing.

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

I think then yes I agree with that.

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

So, what about the minimum set I have there for all – could we say to certify all modules against the following and then we could do the – add the "if" statements to the other privacy and security criteria which are, you know, if you look at spreadsheet the other ones are amendments, yeah, automatic logoff, emergency access end-user devices. So, you could say everybody implement authentication and audit.

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

What if you – Dixie, what if you did it, what if you did it the other way around and for each of the security criteria define when they apply? So –

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

I think some of them – what I'm trying to say is, I think authentication access control authorization column B, column C, column D and column I always apply.

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

Well, but not if you have a service that doesn't –

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

..authentication –

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

You could have a service that doesn't require anyone to ever log into it. I mean, it might be a strange service, but –

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

Well, you still would have to authenticate who is calling it. I mean, even if it's just called by software module you still have to authenticate who is calling it.

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

I don't think that's how people would implement it. I mean, they'll implement a connection to an authentication source. Whatever, yeah, there might be some that apply to all, but I'm suggesting that the matrix of intermediate classifications is probably not going to be flexible enough for employer's complexity so just go straight mapping between security requirements and core functions.

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

Yeah that's what I'm saying, you could – I think you could do that – what I'm – you know, I'm not disagreeing with you guys, what I'm trying to say is, to make it easier I think that there are these four functions – the authentication, access control, authorization, audit and integrity which are really three, four functions, but, you know, they're distributed differently.

I think we could say all the modules have to meet those unless they justify not right? But then for everything else we could come up with these "if" statements like you're talking about. If your module involves PHI then end-user device encryption.

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

Yeah.

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

In other words if your – if it does a clinical, you know, critical clinical function then its emergency access and, you know, we could that for the other three amendments, automatic logoff, emergency access.

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

Hi Dixie, this is Kate again from ONC, I just have a quick question and clarification point. I was wondering how this approach would deal with the situation wherein a provider purchased multiple modules that all had different approaches to the basic material you list under one, you know, how you would rectify them having to re-log in every time they use a different part of their EHR?

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

Well, they wouldn't necessarily, you know, if they implemented single sign-on. Just because it's certified against authentication standards that doesn't mean it can't accept a security assertion that says that the individual has already been authenticated.

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

Well, in –

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

I understand that, but there...

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

There has been –

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

There would certainly be circumstances where they would differ and have, you know, different types of implementation requirements.

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

So, this is what's so flawed about this approach and I don't know that there is any way around it, we're stuck with it so we have to make the best of it, but, this, you know, security is a system function you can't really talk about security absent the system and the systems are as implemented not as picked from a product list.

So, we're trying to certify for security for something in the abstract that could be implemented in dozens of different ways and you're hoping that your certification guarantees that it will be implemented in an appropriate way and there is no way that's possible, it's just absolutely not possible. But the only other alternative is to only certify in-situ systems that have been deployed which is also not possible.

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

Dixie?

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

Well – argue is forget about security and I think that's a bigger risk.

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

Is that really – was the brunt of the argument from Steve's point-of-view is just assume that they do it anyway because we have such a high percentage in the previously certified product and just don't bother with it in the next certification specification?

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

Right, yes.

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

Well, I mean –

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

So, this is Kate from ONC and just to clarify the position we took in the NPRM was such that in our 2014 approach and what we contemplated because we required all base EHRs to include that functionality the majority of modules were already including it and that function ensured that all Meaningful Use providers and hospitals had all the privacy and security requirements.

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

But the thing though Kate that in the 2014 edition you have a complete EHR which is required to meet all the base requirements. What is being proposed, you know, once you've eliminated the complete EHR and the only thing you're certifying are modules and none of them are required to do anything security-wise it is – that would place 100% of the onus on the provider organization to make sure they met base EHR.

Now suppose they go and they buy a bunch of certified EHR technology that either doesn't meet – doesn't have security implemented or doesn't have the right security features implemented, you know, they are not security experts.

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

But, Dixie –

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

Yeah, we definitely understand that it's just the way that the CHPL is set up and that our certification program works is they will not be able to get their attestation number unless the modules that they've chosen meet the base EHR definition.

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

Right, I understand that, I understand that, but what we're trying to talk about here is how we certify products that these people could use, that would be useful to them not how they, a provider out in Kansas City proves that they have a base EHR, you know, the technology should help them do that –

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

Dixie?

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

But –

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

Dixie?

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

Yes?

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

Dixie, I mean, but it's an impossibility. So, let's say somebody comes in and has a module and they use OAuth 2 for their authorization management and they have a beautiful implementation of OAuth 2 and then they go install it at a site that uses WSDL and SAML, well guess what it's not going to work. Both were certified correctly but it's not going to work in the real world.

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

Yeah, but they would just document that David, they would have documented that our interface for single sign-on uses SAML or our interface for single sign-on uses OpenID Connect.

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

Right, but –

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

And they would – and the buyer would know, they would – you know, presumably their technical people would know that, you know, that SAML and OpenID Connect are not compatible you can't use them together for single sign-on. So, they would know that.

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

But –

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

But the way it is now they would know nothing about it.

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

No, they'll – of course they'll know that because they're under HIPAA obligations to meet all these security requirements.

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

No, I mean when they buy the products. The products come –

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

But –

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

It will say, you know, if they have to document how they provide these – how they get these services the product will have documented that they have a SAML –

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

But certifying that a product – certifying that a module picks one particular approach accomplishes almost nothing for the hassle of the certification effort, because the implementer is still required to actually make it work and he may have picked a product that is perfectly well certified for one but it doesn't work with his other product.

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

Right, he shouldn't have picked products that have incompatible interfaces, but what I'm saying is –

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

–

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

When they buy the product, you know, if they take the approach of using one of these three paths they will see what that interface is and you'll see, okay this is a SAML/SOAP interface, this is an OAuth 2, OpenID Connect interface, you know, I don't want two products that are incompatible, but –

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

Yeah, but –

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

Otherwise they'd be buying them with nothing; they would have no insight into what those products do.

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

Well, now, Dixie people don't buy stuff from the vendors with no insight into what the products do and they have them assembled by professional experts who know exactly how to weave these things together that's what we do for a living.

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

Right.

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

This is – we're not talking about a labeling problem here we're talking about a lot of certification effort and I understand ONC's perspective that it may not yield very much benefit at least for those things that require tight coupling to other systems and I think –

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

Why are we certifying them against anything then? Why are we certifying these products at all? Because you could equally argue that, well everybody is going to, you know, capture demographic information why should there be a criterion that says I have to capture demographic information or be a criteria –

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

Well, I think –

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

That says I have to capture electronic notes they're all going to do that anyway. So, why are there criteria there?

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

So, you know, if you want to go down that path I would argue that it makes very plausible argument that the only thing that should be certified is interoperability, but –

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

Well, I would –

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

We're not being asked to answer that question.

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

I would, you know, I would be – I could accept that argument more easily than I can that they should be certified for everything under the sun including whether they've captured smoking status but they shouldn't be certified for security that makes no sense to me.

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

So, the current experience is that 70% are certifying for at least one and even 50% four or more.

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

Yeah but what does that mean? They could be certifying – they could be doing, you know, integrity of the database and nothing else. I mean what does that mean Walter? What does it mean to do authentication access control and authorization, well that's a whole category, no that's a single criterion, they could – let's say they got certified by that but they didn't do audit, it's almost meaningless.

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

Well, I mean, the question is this really, Dixie, I think the question is, first of all one thing is what they call complete EHR and now they refer to as base EHR. I think –

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

Oh, no Walter. Walter you're confused.

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

I think you are confused Dixie because I think your first slide is confusing the criteria in 2014. I think the real question is whether a base EHR should be applying all these criteria across the board in terms of security or whether each module should be and that's I think what they're asking.

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

A base EHR, and Kate I hope you're still there, a base EHR is something that the provider, the person who is meaningfully using the technology has to make sure that the technology that they're using, they're certified EHR technology implements the base EHR. You can't get a base EHR in a product.

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

So –

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

The products that are being certified are modules and it used to be that the base EHR was in the complete module, but you can't get – you can't take a product in and say "I want this certified as a base EHR."

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

This is Kate and the way the certification program works you could potentially bring forth products in a module format that includes all of the requirements of the base EHR definition and have those certified as a package –

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

Yeah.

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

That would still meet the modular definition and be entirely okay for certification.

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

Absolutely, all I'm saying Kate is you can – there's only two types of certification, Meaningful Use EHR module and Non-Meaningful Use EHR module there is not a third called base EHR or a third called complete EHR.

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

Oh, I understand, my point was only to clarify that the –

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

You did.

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

Module doesn't only mean one criterion it could be a group of criterion and could be in fact a complete EHR as we define it today under its capabilities we just won't be issuing that certification title anymore.

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

Yes, yeah, I realize – actually, yeah that would be a good solution maybe, you know, maybe that's what we should say is that they could – you know, maybe base EHRs should be certified, you know, because that is where the privacy and security criteria come in. What do you guys think about that?

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

No, I mean that's in practice how people are going to do it, they're going to purchase most of the capabilities in a base-ish kind of thing just because it's the only sensible way to do it, but I don't think you could write a definition of what that is or require it.

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

Yeah it has too much other stuff in it too is –

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

Yeah, it would be impossible to specify what counts as base. I mean, I think the best we can do is to either say, you know, punt on this and say you're under obligation from HIPAA to do this right you've got to be able to justify if you're audited how you've achieved your whatever the HIPAA term is that I'm blanking on at the moment or if we want we go back and say, each of these capabilities, each of the functions that gets certified has certain security criteria that are implied by that function being present you have to prove that you can meet that through one of our three methods and there's going to be a lot of paperwork and argument, but I don't see any way around it.

You can't refer to a standard. There is no technical specification to test it against. So, you could demonstrate, you know, my module doesn't store any data locally therefore I don't have to have encryption at REST and the reviewer hopefully will say "okay agree" and then you say "my module doesn't ever have, you know, end-user access therefore no emergency access is required" and the reviewer says "I agree."

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

So, what you're recommending I think would be to take the privacy and security criteria and apply these "if then" statements to each criterion?

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

Yeah or – yeah or to, yeah effectively that. I mean, you'd have, you know, logically speaking a matrix of criteria cross against functions and you'd – I mean, it's common sense in 95% of the cases.

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

What did you mean by functions David –

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

Well –

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

I mean, I just want to make sure that functions don't get confused with the functional areas.

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

Well, that's a good question Walter. I'm not being very precise because I don't know what my choices are. I guess really I'm talking about, in my mind's eye I'm talking about technical functionality.

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

Yeah.

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

So, do you store local data, do you ever have users log in, do patients ever have access to this? In other words, yeah, maybe their – maybe it's not the matrix that Dixie had but it's a different matrix that refers to technical implementation choices and for each particular technical implementation choice in that module you have certain security obligations.

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

You know –

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

Yeah, exactly, it's sort of like saying –

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

Yeah.

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

You need authentication; you need to meet the authentication criteria if you do this.

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

Right.

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

If your system does this and a simple statement.

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

Yeah.

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

But not if your system does public health or utilization criteria, or coordination of care “no.”

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

Yes.

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

It's you need authentication if your system does this, if your module does this, you need access control if your module does this. I agree with that.

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

Right, so, Dixie?

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

So, this is Kate and I just wanted to ask a clarifying question. Under this approach would you leave it up to the vendor to attest to the fact that they were not, for example, storing information locally or would the testing body be required to kind of prove that this was the case?

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

I think it's almost unapprovable.

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

Right.

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

That one actually – that particular criterion already has an “if” statement like that I was just going to look it up for you, because it already is – and I think it would be a good example of I think what you're talking about. I'll look it up and I'll read it to you because it's already –

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

Dixie?

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

Yeah?

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

This is Lisa –

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

Yeah, I was just wondering how it would be tested that's all.

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

Yeah.

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

I think where we are right now is, I think David and Walter have a feasible approach and we haven't done the work to do the mapping but it seems to me that it's pretty straightforward to do and see if it works for us, because to me the idea of not certifying any security requirements in an EHR module – it's not palatable to me. So, I'm thinking that we should, you know, try to do that mapping much as you did with your example and see if it works for us.

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

Yeah, this is Kate, all I would ask in support of that is that you guys would give us a little bit of detail about how that testing procedure would go.

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

Okay.

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

So we can fully inform our new path forward.

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

Well, given that we're not using standards here it's a little difficult to decide how to test that's why some of this certification is so painful.

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

Yeah, I completely understand that's why we'd like as much guidance as possible, but I also understand your limitations as well.

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

Okay, if you look at, see the EHR end-user device encryption already says for example that these paragraphs must be met to satisfy this criterion it's end-user device encryption. EHR technology that is designed to locally store electronic health information on end-user devices must be – must encrypt the electronic health information stored on such devices after use of the EHR technology on those devices stops. So, you would have to – you would want to rephrase every privacy and security criterion to have that same sort of situational flavor to it.

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

And do most of them have that Dixie or is it just one?

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

No, I think that's the only one. Let me look at some of the others, let's see – like here's – no I think that could be the only one that has that kind of a sense to it. Yeah. So, we would essentially build in the "if" statements into the privacy and security criteria. I mean, essentially, yeah, I'm not saying literally, but that's what you're saying, right?

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

Yeah, I mean, this is David, I'm not quite sure what the right descriptive name is but it's an implementation, it's a functional or technical implementation that raises certain security requirements and we could enumerate what those are for those requirements that have some optionality to them.

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

Well –

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

But, I'm not sure that's going to make it easy to test them.

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

Right, but that's a common problem with a lot of criteria, you know, that don't have standards attached to them. They're functional, they're tested functionally.

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

Yeah, that's why we should be certifying to interoperability and leave it at that, but that's not our call unfortunately.

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

Yeah, so, what we're saying, I think – and we would still give them these three paths, but these "if then" statements would go away, statements one through four would go away and we would recommend and maybe do an example, maybe use the end-user encryption as our example, that these – that the criteria themselves should describe under what circumstances that function is needed. Is that right?

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

I think so.

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

I think so, yes.

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

And if we did that then every module would be certified against every privacy and security criteria because some of them would just be N/A because of the way the criterion was stated. Right?

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

Yeah, I –

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

Technically, yes.

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

The devil is in the details.

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

I know.

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

And under this approach how would we deal with situations where, you know, the implementation of those requirements were done differently and maybe in a conflicting way?

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

Well, we wouldn't. We would – I think that the path two is our recommendation for, you know, helping to make sure that there – you know, that these modules are integratable not so much interoperable, but integratable. Anybody else? See, the certified EHR technology list, whatever it's called, CT whatever –

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

The CHPL?

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

The CHPL, yes, yeah, it mentions what products are being certified against so you can already see, you know, if you have a Cerner's suite of products, you know, they already will say – and any module in there would say, here's what I used for security.

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

Dixie?

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

Yes?

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

This is Peter, I'm sorry I tried to talk before but I forgot that my phone was on mute. I just wanted to comment on the comment earlier about the modules that might have different – use different technologies for their privacy and security and that smaller practices don't want to have to use a consultant to put these pieces together some of them might have a kind of techie doctor, but techie doctors tend not to be that good that they understand a lot of this different technology.

If it's going to be done individually we might want to have some sort of a standardized terminology for or standardization to disclose the type of technology you're using for your privacy and security. Do you understand what I'm saying? That, you know, a lot times people won't really know the differences between the different modules and be able to figure out immediately that they are incompatible. So, we might want some way of mentioning that so they can determine it themselves.

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

So, how would that be captured, would that be captured in the – I guess in the system documentation which is required for certification.

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

I mean, this is David, I think that happens, you know, today already it's not simple and security is obviously incredibly complex and getting more complex every day, but there is no way to take something that complex and make it just brute force simple unless you have a single vendor implementation where they control everything.

So, I think that there are families of approaches today that work well together and people that put systems together just need to understand what those families are and how they work and then ask the vendors to assure them that it will work with the other products they already have and put the burden on the vendor to sort of say "yes, well we support that and we'll make it work or not."

I don't, I mean, there isn't a, you know, unless you wanted to require everyone to use a particular IHE profile and even there is so much optionality you probably wouldn't get what you wanted.

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

Yeah, the thing is these small practices generally use a single product anyway, integrated product that everything is integrated.

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

Right but if a small practice wants to buy an EHR that doesn't include ePrescribing and they want to buy that from someone else then ask the two vendors to assure they work together and the vendors can figure that out in a heartbeat.

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

If they have the right information.

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

Yeah, but the vendors will figure that out, I mean, that's what we do every day, all day long.

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

Yeah that's true.

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

We get on the phone and figure it out.

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

Yes.

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

Or they'll write a, you know, whatever. I mean, it's just – since we don't have a standard to measure against we can't certify against that standards nor can we require it for deployment we're just – we're not there industry is not there.

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

Okay. Okay, so do we want to do an example or do we want to, you know, do a spreadsheet like some of you have mentioned, you know, I don't know exactly what would go down the side. If we did a spreadsheet like what I have, the nine things at the top are the privacy and security criteria, so how – what would you –

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

Well, how about if you worked it backwards Dixie and said, you know, for each of the security criteria what are the functional attributes that would trigger the applicability of that criteria?

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

That's what I'm saying or trying to say, yeah.

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

Yes, so let's just make that list and see how much overlap there is and then you've got your criteria.

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

How much overlap there is among –

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

Well, I mean, in other words list it for each security, build a list for – take each security criteria on its own, list the things that would trigger it and then see – add those lists together, reduce for the duplicates and there is your matrix.

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

I see, yeah, you lump them together in other words?

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

Yeah.

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

Yeah.

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

After you've – you know do it bottom up in other words, you pick each criteria, list the things that would trigger it and then say "oh, look this one shows up in every single one of them." So, that's, you know, problem one –

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

Yes.

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

In the matrix and we'll give it a name and – I mean, it may not be that hard to do, it may turn out to be impossible I don't think we'll know until we try.

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

Okay, do you want to take a stab at it?

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

No, I've got a real job to do.

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

Hey, Walter, do you want to work together to try to do a first draft of this?

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

Yeah, I guess that would be fine. I mean –

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

And I'm happy to contribute, I didn't mean that I'm not going to help, I just – I don't – let's start a – let's circulate something and add to it. Unless, Dixie, can you think of something that already exists out there in non-healthcare standard space that we should start with? I can't think of anything, but, you know that space a lot better than I do.

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

I mean, in most domains you wouldn't have the variety of functional – of functions that we have here.

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

Right, but is there some kind of a security capability check list?

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

There might be, you know, there might be a NIST thing that – what is the NIST 800-53?

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

Yes –

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

Is that right? Yeah, the 53.

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

Dixie, I think we can find something and I think we can – you know, going through the exercise is going to be very informative so I think we should, you know, try to do that circulate it around and see what we come up with.

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

Yeah.

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

I would just try to keep it simple rather than –

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

Right.

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

Try to detail to the maximum granularity level –

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

Right.

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

All the possible scenarios, otherwise, it's never going to end.

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

That's right.

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

I think we could keep it at a high level and see what it looks like.

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

Yeah.

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

Yeah and to the extent perhaps you guys can at least provide some recommendations for how like each of those functions might be tested or at least, you know, overseen through testing that would be greatly appreciated.

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

Okay.

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

And if we can't come up with something does that mean that we don't have to be tested for them?

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

Well, I mean, it just is worrisome to me to create a situation that you can't test and then you're just kind of hoping that the vendor has represented everything honestly and having no way to verify, you know –

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

I mean – I think Kate that's a reasonable request and we could at least visit, you know, whether we can conceive of a way to test it and, you know, I think that will be informative too.

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

Well, we aren't – we aren't recommending any new test it would be the same criteria –

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

Right.

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

This matrix would just define when the module has to conform to it. So, the testing – it shouldn't be any different than what you're already – well, that's right you're not doing anything.

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

Yeah, so you'd have to have some way to verify whether or not the like kick start is present or not present.

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

Yeah.

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

Whether the function is there or not.

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

And even whether – and even what would determine whether the documentation is – documentation of the interface is acceptable.

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

Right.

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

Yeah.

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

Exactly.

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

Yeah, yeah, yeah I see, yeah. Okay. All right, I think we have a solution here and how long do you think it will take you guys to give us – why don't we schedule another – I think we have another meeting scheduled or on hold or something don't we Julie, the 18th or something?

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

Hi, this is Julie, that's right, Dixie, we have the 18th that you have slated for the NSTIC discussion if needed, but if not we can use that as a follow on to this call and then I do have the 23rd on hold.

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

Yeah, the 18th is Good Friday, so I won't be available.

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

Okay.

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

A lot of –

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

Okay.

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

So, why don't we just off line work out a date where we can get together and just talk about this.

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

Okay.

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

And when do you think you could have – now it doesn't have to be an exhaustive perfect list but something where we can at least satisfy for ourselves that it can be done that it's feasible?

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

I mean, I think, you know, the 18th would have been reasonable and maybe, you know, Walter and I, and David can work on it, you know, we'll schedule a meeting that works for everybody, but, you know, either the 17th or the early the following week.

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

Okay, okay you can work with Julie to just set something up.

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

Well, see if we already have the 23rd why don't we use the 23rd?

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

Yeah when –

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

Well, I can't be there, that's the day a lot of people I would think, anybody coming to the – the Standards Committee is the next day.

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

Yeah it's a travel day.

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

And we really need something to report back, but we can report back status that would be fine.

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

I think we can find the time hopefully at least Julie can try.

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

And just to reiterate the comment period closes on the 28th so that is a hard stop.

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

Okay.

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

Yeah.

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

Well, at the very least we can – we can do our comment, you know, as a status, you know, marker but let's target the 28th. Okay. Kate is there anything else you need us to consider?

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

Not at this time but I will circle back with Steve and make sure that you guys get any additional information that he thinks would be helpful.

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

Okay. Thank you. Thank you for calling in too.

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

Sure.

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

Okay, anybody else? Okay, I think what's our next item on the agenda just next steps?

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

Dixie you broke up there.

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

Oh, the – Julie, the next thing is to just summarize and close, right, on the agenda?

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

Yes that correct and just so I'm clear, the meeting that we're trying to set that's not the 18th and the 23rd it's just like an internal meeting to see if that matrix works right?

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

Yeah.

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

So, I'm going to try and coordinate Lisa, Walter and David schedules?

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

Yeah.

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

And Dixie.

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

And Dixie, okay, I will do that.

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

And we probably at that same meeting Julie should, you know, we should have a draft of our, you know, of the words we want to put in our NPRM response instead of what we were planning.

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

Okay.

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

Even if we don't have the full details we'll at least have the, you know, here's what we would like to recommend so that we can – you know, we'll have a draft there.

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

Okay.

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

It will be just one, you know, one or two sheets, probably two slides in that package you're preparing.

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

Okay.

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

Okay. I would like to encourage all of you to look at the NSTIC slides and get back to us with any comments or suggestions you have, otherwise we're going to move ahead with what we have and the next thing you'll see is an announcement for a meeting to talk about this last area for the NPRM. I think we will be able to distribute, I'm sure we will, our draft NPRM slides as well for review before that final meeting. Okay, thank you, thanks everybody for dialing in today we really appreciate, this was a good discussion.

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

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

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

We need to open it up for public comment.

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

Yeah, I was going to ask about that, yeah.

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

Yeah.

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

I think we still have open –

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

Yes we do.

Public Comment

Rebecca Armendariz – Altarum Institute

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

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

Okay, well thank you everybody, have a good weekend.

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

Bye.

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

Bye.

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

Thank you.

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

Bye.