

HIT Privacy & Security Tiger Team
Draft Transcript
April 9, 2012

Presentation

Mary Jo Deering – Office of the National Coordinator

Good afternoon, everyone. This is Mary Jo Deering in the office of the National Coordinator for Health IT, and this is a meeting of the HIT Policy Committee's Privacy & Security Tiger Team. It is a public call and there will be an opportunity for public comments at the end. I'll ask the members to identify themselves when they're speaking for the transcript that's going to be made. I'll start by taking roll. Deven McGraw.

Deven McGraw – Center for Democracy & Technology – Director

Here.

Mary Jo Deering – Office of the National Coordinator

Paul Egerman

Paul Egerman – Software Entrepreneur

Here

Mary Jo Deering – Office of the National Coordinator

Dixie Baker

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Here.

Mary Jo Deering – Office of the National Coordinator

Dan Callahan? Neil Calman? Carol Diamond?

Rebekah Rockwood – Markle Foundation – Manager, Health

This is Rebekah Rockwood for Carol.

Mary Jo Deering – Office of the National Coordinator

Judy Faulkner

Judy Faulkner – Epic Systems – Founder

Here.

Mary Jo Deering – Office of the National Coordinator

Leslie Francis

Leslie Francis – University of Utah College of Law

Here.

Mary Jo Deering – Office of the National Coordinator

Gayle Harrel? John Houston? Alice Leiter?

Alice Leiter - National Partnership for Women & Families

Here.

Mary Jo Deering – Office of the National Coordinator

David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

Mary Jo Deering – Office of the National Coordinator

Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Micky Tripathi?

Micky Tripathi – Massachusetts eHealth Collaborative – President & CEO

Here.

Mary Jo Deering – Office of the National Coordinator

Latanya Sweeney? Alright, would staff who are on the line please also identify yourselves?

MacKenzie Robertson - Office of the National Coordinator

MacKenzie Robertson, ONC.

Kathryn Marchesini

Kathryn Marchesini with the Chief Privacy Office within ONC.

Linda Koontz – MITRE – Principal Information Systems Engineer, Privacy

Linda Koontz from the MITRE Corporation.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Joy Pritts, ONC.

Mary Jo Deering – Office of the National Coordinator

Okay. Back to you Deven and Paul.

Paul Egerman – Software Entrepreneur

Great. Thank you very much, Mary Jo. This is Paul Egerman, and I want to welcome everyone to our Tiger Team meeting this afternoon, and tell you a little bit about what we will be doing. The Tiger Team, first to remind everybody, is really sort of a subcommittee or a task force or a working group of the HIT Policy Committee. It consists of members from the Policy Committee and from the Standards Committee and from other experts that we've been able to recruit to help us. What we will be talking about, in general, is to continue our efforts to reach agreement on some comments to be provided on proposed rules.

To refresh everyone's memory, we've had a number of meetings. We made a number of recommendations and an NPRM was issued, basically just related to the proposed rules for Stage 2 of Meaningful Use. We felt very good that many of our prior recommendations were included in the NPRM, but there are some places where they were not included. What we are trying to do is say, "Where do we want to make recommendations to the HIT Policy Committee that will be meeting on April 4th, in terms of things that perhaps we want to review where our recommendations were not included in the NPRM?"

We need to finalize any comments or recommendations we want to make to the Policy Committee for their meeting on May 2nd, and also, just to remind everybody, we only have this meeting and one on April 23rd. We only have two other meetings left before May 2nd.

That's sort of a general overview of the discussion, and also, the previous recommendations that we made that were not adopted in the rules; here is a quick summary. There are the issues related to patient portals. There are some issues related to EHR modules; ePrescribing of controlled substances; digital

certificates; and also some recommendations we made on patient matching. Those are the areas where we are going to have discussions today and in the next meeting to see whether or not we want to comment any further. And to ground our discussions we will be mainly reviewing what we said before, compare that to what's in the NPRM, and then see if there's anything we want to do to bridge that difference.

Let me ask you, Deven, before we start on patient portals, does that summary look right and—

Deven McGraw – Center for Democracy & Technology – Director

Yes. Perfect, Paul. It's terrific. Yeah. So we're going to try and get as far as we can on this call, maybe even all the way through the remaining recommendations, which would be terrific. We'll do the best that we can. The first issue to discuss is whether we want to say anything additional on patient portals, and over the next couple of slides there are four recommendations, most of which are really directed at certification of EHR technology in terms of what elements we had previously recommended would need to be included and they were not in the proposed rules. The two that are on this slide involve recommendations that we made about testing certified EHR technology for authenticating patients using at least a single factor and the ability to do a secure download for the view download transmit or portal functionality. This recommendation, which we had previously made, was not accepted by ONC. What they said in the proposed certification rule was that such technical implementations are commonplace and ubiquitous and therefore don't necessarily need to be required for certification purposes. And we had also recommended that certified EHR technology include a capability to detect and block programmatic and unauthorized user attacks. This was one where the Standards Committee felt that this recommendation might be a good best practice but was likely to be surpassed by innovation in the field of authentication. Obviously, with folks from Standards on the line we can get some clarification about what their thinking was here.

But neither recommendation that we had previously made was adopted so really our options here are to reiterate them if we think it's still worth doing. We could make no comment at all and say, "Well, you know, we put those up there but they didn't think that it was worth including when we had specific reasons for one and we know the Standards Committee suggested a different approach for number two." And then, the other option that's in the middle of our options for comment is to ask the Office for Civil Rights, which oversees the HIPPA Privacy and Security Rules, to issue some security rule guidance on portals. Obviously, any covered entity or business associate on behalf of a covered entity that is providing this functionality for a provider participating in Meaningful Use would be covered by those rules. And it might be helpful for them to have some guidance about how the security rule can be appropriately applied to the portal functionality, which was not something that we recommended the first time around but arguably might be a way to get more guidance out to providers on security issues without specifically stating pieces of technology that we think ought to be included in certification.

With that, I'll open up the floor for discussion, and Paul and I offer options for consideration in terms of our recommendations but we're not necessarily limited to the ones on the slide.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie. I can briefly talk about the first one. The Privacy and Security Standards Workgroup also noted that not only authentication of patients but for viewing and downloading EHRs, the NPRM doesn't include any security requirement at all, criteria at all. And we believe that was an oversight because they included security for forwarding a document to a third party but they completely neglected addressing security for viewing and downloading. And we recommended that something similar to secure messaging be adopted for viewing and downloading, which we would be authentication of the patient if secure messaging included authentication of the patient, encryption, and integrity protection of the link.

Deven McGraw – Center for Democracy & Technology – Director

So let me ask you Dixie, this is Deven, isn't this functionality required to be in the Base EHR, which would be required to demonstrate the certification requirements that were, at a minimum, required in Stage 1 and are required to be in the 2014 criteria as well?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, even if it—yes, they are required to be in the Base EHR but there's no requirement that the patient interactions use this or anything else actually; that these patient interactions use these capabilities in the Base ERH.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. But the requirement to use is really a policy issue, which arguably one could say was covered by the security rule requirements to adopt certain physical, technical, and administrative safeguards, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No. No. There's no requirement to—what you have here, required testing and certified EHR for authentication of patients, right now there's no criterion that says you must authenticate a patient before they view or download a record. There's nothing there that says that.

Paul Egerman – Software Entrepreneur

So let me see if I understand what you're saying Dixie. What you're saying has two parts, getting back to what's on this screen. You're saying you think there should be authentication even though the NPRM said we don't need to do that because our independence ubiquitous and you're saying something further. You're saying that secure messaging specifications or requirements should be applied to view and download and they were simply inadvertently missed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yeah. Because there is a criterion that says that for secured messaging with a patient you must authenticate the patient and you must integrity protect and encrypt the data. It says that. The NPRM says that. It does not have anything comparable for viewing or downloading.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

This is Joy and I would like to point out that some of the policy here is covered by the security rule. I'm going to say it was as a technical safeguard in the security rule there is a standard which requires person or NC authentication and requires public entities to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. I think that there's been kind of a recurring theme throughout this process that we saw in the first Meaningful Use phase as well with kind of hesitancy to re-iterate policy that's already in the Security Rule unless there's a really good reason to. There was a really good reason to for the encryption piece because I think the members of this workgroup concluded based on their review of what was imported in the breach notifications, and that piece of the security rule did not seem to be being necessarily followed to at least the spirit it was intended.

Here there are two pieces. One is we were having a hard time—I personally have a hard time seeing how you can authenticate anyone without using at least single factor—how you can provide access to a portal without at least a password.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I understand what you're saying Joy and Deven. I understand that they don't want to—but they're not being consistent. Like if you look at row 20 of the review. Well, maybe you aren't looking at this. Well, you might be, I don't know. But at any rate, the criterion 170.314(b)(1) is authentication access control and authorization. So somehow they deemed that was important to include as a criterion and this is verified against a unique identifier user name that a person seeking access to EHR is the one claimed, and establish the type of access to electronic health. Now, these are for authenticating oneself to the EHR itself but they don't have a similar requirement for patient access. How did they choose that if you are authenticating yourself as a user of the EHR itself that merits a criterion but if you're a patient accessing your own information through patient interaction that doesn't merit authentication access control?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

This is Wes. I wonder why you are singling out the patient as being different from any other user here.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Because they did. They have a whole different set of criteria. They have to provide patients the ability to view online, download, and transmit their health information within four business days of the information.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

But they also have HIPPA security criteria that talks about users, right? Aren't patients' users in that case when they're viewing or downloading?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

So why do they need this separate criterion that says—to me they're the same thing. Do they also have a criterion that says, "Provided users the ability to view online, download, and trans—"?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No. I don't think it's important. I mean, you can have a discussion on whether that's important or not, but clearly the Policy Committee was driving this specific requirement towards patients not towards other users. I want to say that as I've gotten to know a lot of what goes on through Gartner in terms of what banks and other companies do to make single factor authentication work it's a continuing moving target. I mean, it's not just that you put in a password and it's encrypted and they check the password. They have many defensive activities that are going on.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But that's not what we're talking about, Wes. It doesn't say—right now it doesn't say that they need to authenticate themselves at all, and I don't think anybody—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

But users need to authenticate themselves. These are users. I don't see the problem. One of the other people who's on the call has actually said that, "I say if a regulatory body suggests the regulation is not needed, we should grab it and be happy." I agree with the general notion that no provider is going to put up a system that doesn't authenticate their patients in terms of downloading data. They have too many vulnerabilities under HIPPA, plus they understand the ethical responsibility. I'd love if my providers were as easy to get to as Bank of America. I'd love it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, I—

Paul Egerman – Software Entrepreneur

Wait a second, Dixie. So, Wes, what you're saying is, if I'm hearing you right, is we just focus on what's on this screen in terms of issue of single factor authentication. If I heard you right, Wes, I want to make sure I got it right. You're saying what's in the NPRM is fine. In other words, you don't think that we need to make any—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes. That's what I'm saying, yeah.

Paul Egerman – Software Entrepreneur

Okay. So what I want to find out—I know you're not quite there Dixie—I want to find out is anybody else on the call who agrees with Wes or agrees with Dixie on this issue?

Rebekah Rockwood – Markle Foundation – Manager, Health

This is Rebekah. I think Wes' point is really important and I wonder if in our recommendations we could just clarify that we assume that a user includes the patient so that the general certification criteria for authentication would include authentication for the patient portals and the secure communication and other things like that.

Deven McGraw – Center for Democracy & Technology – Director

This is Deven. I'm inclined to agree with Wes although I do think it would be helpful for there to be security rule guidance on this particular point but not necessarily to need anything additional on certification. I get your point Dixie about the inconsistency but the reality is what do we think is needed in certification that we don't think would otherwise, absent a hard requirement in certification, would actually be there? And I'm convinced that the current legal obligations are sufficient to drive the use of the sort of basic security measures around authentication that we think need to be there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

If that's the point we want to take and I can be persuaded to take that way, but if that's what we're going to argue then I think criterion number 20 should go away, the authenticate central and authorization, because it's already covered by HIPPA it shouldn't be there then.

Paul Egerman – Software Entrepreneur

Well, let's do these things one at a time. I just want to make sure we get through the list of what our recommendations were and those variances. It seems like we're in agreement on the first one, which is that we're really not going to make any additional comment on it. In other words, the reason I personally like this is the recommendation for single factor is really sort of like at the lowest level recommendation you can make for authentication, and picking up on what Wes said, a lot of people are doing a lot of other things that are more creative than what we recommended. So if you actually put in certification criteria for something that is very simple that action may discourage people from doing something that are a little bit better because it actually gets harder to test against the simple case.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Why would they do something harder if there's no criterion for it to begin with?

Paul Egerman – Software Entrepreneur

Well, they would do something harder because they ultimately want to do a good job. I mean fundamentally the cost of the certification should be like a minimum base level, and hopefully a competitive environment will be something that vendors and users will want to do some pretty new things. I liked what Wes said about how the banking systems are changing how they do things and maybe some vendor will have a better approach that's more than one factor for patients that will work well.

Leslie Francis – University of Utah College of Law

This is Leslie Francis. The proposal doesn't say only single factor. It just says at least single factor.

Paul Egerman – Software Entrepreneur

That's right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And the criteria don't even say at least single factor. The criterion says nothing about it. That's the point I think we should—it doesn't seem to be getting through. It just doesn't seem to say anything about it.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

This is Joy. I have a question. So if you did not have single factor authentication wouldn't the provider essentially just be opening all of their records to everybody? And nobody does that in almost any kind of Internet application. So what are you getting for adding it here? Nothing.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, then what's to be gained by adding it for EHR? Everybody's going to do it because they have to meet HIPPA. I think the inconsistency suggests that it's not required for patients because if you say, "Well, HIPPA requires entity authentication so we don't have to say it in the criteria," then why is there a criterion that says, "Authentication, access control, and authorization for EHRs"?

Paul Egerman – Software Entrepreneur

So here's what we can do—I've listened to all of this—we can also report that there are some disagreements. I mean, it seems like some of us think this is fine. I know Dixie you want—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I want consistency is what I really want.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. I don't think they meant to be deliberately inconsistent Dixie. I think that these rule makings happen often in a bit of a rush. We do have a consistent legal obligation on the books to authenticate users, and it just so happens that in one circumstance there's a certification criteria expressly requiring the testing and it's absent in another doesn't necessarily mean the absence of a legal obligation to authenticate anyone who is coming in to a record that has legal obligations to protect it.

Leslie Francis – University of Utah College of Law

Yeah. This is Leslie. That makes it really important to clarify the patients are users.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think we can all agree that a comment requesting that it be clear, that there be language at least in the preamble that makes it clear that patients are regarded as users is valuable. I think that considering not only is there a whole lot of energy required to get out a draft or a final regulation but that we're looking at some criterions that were created some years ago and some criteria that are new. I think that pushing for consistency for consistency sake, although desirable, is probably lower on our priority than getting through the list.

Paul Egerman – Software Entrepreneur

I agree because I look at this and we're about 1/3 of the way through our time on the call and we haven't finished the first item. So it seems to me that there is some general agreement on leaving this alone but also perhaps making some comment about this issue about consistency and users, and so we'll try to draft something. If this works okay for you Deven, can we go onto the next one, the second recommendation?

Judy Faulkner – Epic Systems – Founder

This is Judy. Can I mention one thing? I think it's not only—I think we have consistency versus prescribing too much, prescribing what's already being done, and when you think about it it's not just our time getting through it but everybody else in the whole country who has to read it and work through it, has to spend time on every issue, and if we can cut out those that are more obvious I think it will help everyone.

Paul Egerman – Software Entrepreneur

Okay. I agree. That makes sense. Let's go on to the second recommendation here, which had to do with detecting and blocking programmatic and unauthorized user attacks. Basically, that did not make it into the NPRM, and so our options are similar. We can make no comment. We can put it as guidance, or we could say, "Hey, this is really important, that we want to re-iterate on it." I'm taking a guess—they didn't say in the NPRM why they didn't include this.

Deven McGraw – Center for Democracy & Technology – Director

Yes they did.

Paul Egerman – Software Entrepreneur

Oh, what did they say?

Deven McGraw – Center for Democracy & Technology – Director

Yeah. They said the Standards Committee disagreed with us and they agreed with Standards, and the rational, which I summarized Dixie and I hope I did it justice, also Wes and David, this is an issue of assurance of proper authentication of anyone who's attempting to use a portal. And our idea was a particular approach to blocking unauthorized people from being able to access the portal, but the reality is that the technologies for authentication are rapidly changing and it didn't necessarily make sense for us to specify this particular solution to be required in certification.

Again, it maybe arguably goes to the issue that we just talked about, which is there already is a legal obligation to authenticate users, and assuming we make clear that we think users in this case also include patients the expectation is that providers will have to step up to the plate with a combination of policies, best practices, and technology solutions that they can work with their vendors to provide. I thought it was a good idea at the time but I see why it was rejected, quite frankly.

Paul Egerman – Software Entrepreneur

Yeah. I do too. My question is, is there anybody who wants to argue for re-iterating the recommendation? So I'm assuming silence means everybody is okay with making no comment on this or it means that I didn't wait long enough, one or the other.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I'm okay leaving it alone. I think it's very similar to the one we just discussed. These are best practices that evolve rapidly with technology and are covered under the Security Rule from a legal point of view already.

Deven McGraw – Center for Democracy & Technology – Director

Do we want to add that we think it would be helpful for the Office for Civil Rights to be providing some guidance on the applications of the security rule to this particular context? Not these issues of blocking programmatic attacks but having them provide helpful guidance to providers about how their legal obligation under the Security Rule can best be met for this particular use case. It would be sort of bully pulpit. Again, we don't advise the Office for Civil Rights.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So this is the notion that a consumer facing portal creates new risks that should be called out with specific guidance; that would be the essence of it?

Deven McGraw – Center for Democracy & Technology – Director

Yeah. Maybe not necessarily new risk but maybe they are new risks, but this is a different function for many healthcare providers who've never provided this before and that the security rules will apply and what are some practical ways of meeting those obligations for them?

Rebekah Rockwood – Markle Foundation – Manager, Health

This is Rebekah. I think that'd be very helpful guidance as long as it can be made easily accessible, and if they do develop it perhaps it's a tool that places like the regional extension centers could use in their work. I wonder if it would be beneficial to have guidance for patients as well.

Deven McGraw – Center for Democracy & Technology – Director

Well, we already did that. That got through the transparency recommendation.

Rebekah Rockwood – Markle Foundation – Manager, Health

Well, then I take that back. Yes, I really like this idea.

Paul Egerman – Software Entrepreneur

So instead of OCR guidance could it be ONC guidance in terms of guidance, in terms of for EDs for purchasing, and also, there would be guidance that extension centers could get it out, which is find out how this occurs, the programmatic blocking occurs.

Deven McGraw – Center for Democracy & Technology – Director

We call it technical advice, Paul.

Paul Egerman – Software Entrepreneur

Yeah. So in other words, that could be done on the ONC side. It's basically technical advice about purchasing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It wouldn't surprise me if NIST already has something that could be leveraged for this purpose. This is David. It certainly seems like this could be helpful and certainly would not be harmful other than the fact that it's more work for somebody.

Paul Egerman – Software Entrepreneur

Okay. So it seems like we have some sense of consensus that we're not going to make any NPRM comment about recommendation number two, but we are going to give some suggestion about guidance.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

You know, we already—as Deven said, we already provided a lot of guidance about patient portals. Maybe we just add this to that guidance.

Paul Egerman – Software Entrepreneur

I think that makes sense. Okay, are we ready to move on?

Deven McGraw – Center for Democracy & Technology – Director

I think we are Paul.

Paul Egerman – Software Entrepreneur

Great. Number three.

Deven McGraw – Center for Democracy & Technology – Director

So number three; this was a—we had a recommendation requiring certified EHR technology to include requirements for data provenance that can be accessible to the patient or user. Because the consolidated CDA does have data provenance in the header one of the options for comment is to assume that this recommendation was addressed by that requirement; the CCDA with the data provenance in it, if we think, in fact, that suffices; or if we don't, perhaps to re-iterate the recommendation; and then, of course, we also have the no comment function.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. This has been one of the pet peeves for me, but I think what's missing is the need for a digital signature for integrity validation not for non-repudiation. It could be a system-wide digital signature, but the cost and complexity of adding that is nontrivial and I think it's probably a non-starter in the debate. But to me the risks that a consumer runs by managing their own copy of this data is that downstream re-consumers of the data, people that they forward it to or share it with might not trust it. And if the data has been in the hands of the consumer in the form of a piece of text be it XML or with a CDA header or not it obviously can't be trusted in any kind of meaningful sense.

The workaround for that today might be that you have the provider transmit the data directly to the receiver over a secure channel like Direct in which case you trust that channel has protected the data and it hasn't been in the hands of someone who could tamper with it. I think what's missing is the digital signature, but I doubt if we could push that very far.

Paul Egerman – Software Entrepreneur

So what are you saying though? Are you saying that we should re-iterate our recommendation? Do you think it's already addressed by CCDA? What are you saying about this?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, I'm saying no. Unfortunately, since it wasn't proposed I suspect we'd have a hard time adding a requirement. I don't think the CCDA has solved this problem at all because it's an unsigned piece of text. The problem is, however, adding something complicated like that at this point is probably an uphill battle. Maybe Joy would comment to tell us, but there's a fair amount of complexity with digital signature. We've touched on that with the certificate of request for instance.

Paul Egerman – Software Entrepreneur

The digital signature is not the same as provenance.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, it's part of provenance.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

It's related but it's not on point. I think you'd have a hard time saying that you really raise the issue of digital signatures by raising the issue of data provenance. They're related but they're not co-extensive. I don't know the answer. In all honesty, I don't know but I think that it might be a little difficult. I'm not saying it's impossible but it's not on point. It's not clear.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie. I think digital signature is included in this requirement because the requirement, I think, we're talking about here is powered in EHR data to a third party, and the NPRM criterion or standard for forwarding data to a third party is Direct, and Direct has a digital signature.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. But that doesn't—the question here is posed as consumer access to it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yeah. But even for consumer, you know, whenever a consumer request that it be sent to a third party whether it be a PHR or anybody it still has to use Direct and Direct has a digital—

Paul Egerman – Software Entrepreneur

The problem—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. If you send it to me and I tamper with it and then send it to you with Direct, Direct has added no value and yet it's still been tampered with.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yeah. But the criteria only addressed an EHR to a third party, and they don't go beyond that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

This is Wes. I think that David is addressing a very important point that is beyond the scope of the NPRM. I would like to suggest that the assumption that all header data in a CDA document will be displayed to the patient is not an obvious assumption. And so I think that there is a direct comment recommending that there be a certification requirement that the provenance data be displayed as part of the display of the CDA document. I think, in general, there is language that says everything in a document must be displayed, but I can see an awful lot of people sort of going light on displaying some of the header elements that seem to be more historical than relevant.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, you know, when I received Deven's question about this several weeks ago I looked up the CCDA specification itself and even there it says, "We recommend that the header information be displayable." But it isn't part of the specification that it be displayable.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Oh, you looked in the CDA or the CCDA that comes ...?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

CCDA, yeah. It recommends but it's just specifying the standard. I'm agreeing with you here.

Paul Egerman – Software Entrepreneur

So the sense I'm having is people want provenance but they don't see how we can do anything based on where we are right now.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No. I think the sense is there is language right now in the certification NPRM Standards and Certification that requires that all of the CCDA be displayable to a person whether or not—actually, that language may be in the proposed. It may be proposed though.

Deven McGraw – Center for Democracy & Technology – Director

It should be provided in human readable format and that is in the proposed rule.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay. So I think that although it might seem redundant actual practice to-date is such that it's worth mentioning explicitly that the header data related to provenance must be included in the data that is viewable to a human user.

Paul Egerman – Software Entrepreneur

So your suggestion is that we just add that as a recommendation as far as a clarification that the

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yeah. As long as we're comfortable—and I haven't verified it myself but it sounds like other people have—as long as we're comfortable that the data in the CCDA header does, in fact, match our recommendations for provenance.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. And we didn't actually specify what provenance would look like. That the patient be able to see the the, you know—

Paul Egerman – Software Entrepreneur

So the recommendation is that the NPRM is fine as long as the requirement to display the header information includes the display of the provenance information that's included in the header information.

Deven McGraw – Center for Democracy & Technology – Director

I wonder if we could make this even simpler and just say that the provenance information has to be viewable to the patient in human readable form or it will probably be in the header but—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. I think you'd be at risk of over engineering user interface design if you specify when and where it should be readable. I think that the human readable and present are sufficient.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yeah. I think that's much better.

Deven McGraw – Center for Democracy & Technology – Director

That's terrific. I agree with that.

Paul Egerman – Software Entrepreneur

It seems like we have an agreement on number three.

Deven McGraw – Center for Democracy & Technology – Director

That's great.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I'm still holding out for digital signature in the future but I'll save it for Stage 3.

M

You don't want to discuss it some more now, David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, if you really want me to.

Paul Egerman – Software Entrepreneur

Moving on to number four.

Deven McGraw – Center for Democracy & Technology – Director

So number four, now recall—and I recommend that we just chat about this for a second—that we did have recommendations about guidance to providers and hospitals to enable them to be transparent with patients about the benefits and risks of using portals. This guidance was mentioned only briefly in the NPRM, and we didn't ask for it to necessarily be required as certification. In fact, we said it shouldn't be required as certification best practice guidance. I think the only question is whether we use this bully pulpit opportunity to urge ONC to more formally endorse our guidance recommendations and develop and implement a dissemination strategy so by the time some of these portals are in more robust use by 2014 that providers are aware of it and ideally using it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I support what you said particularly because this really isn't a certification requirement.

Deven McGraw – Center for Democracy & Technology – Director

It's not.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

This is Joy. I have a question. Are you going to then have—it sounds like you have two separate things going on here. You have a list of items that aren't really certification criteria that you would like to make recommendations on, and then, you have a list of recommendations that you'd also like to make. Is that right? I mean, I'm trying to think of what your process is here going forward.

Deven McGraw – Center for Democracy & Technology – Director

So there will be a letter, a comment letter, I assume, coming from the Policy Committee directed towards CMS and ONC for the respective proposed rules; Meaningful Use and Certification. And we've got some things that we have decided that we want to include in comment to those specific proposed rules, and those, of course, would be appropriate for that letter.

For the couple of items where we have identified say that ideally more guidance whether it's guidance from the Office for Civil Rights on the Security Rule application or technical guidance from ONC about how a provider can be a good purchaser of security for its EHR and the portal functionality in particular, and then urging you to do something with the guidance recommendation that we issued, that might have to be in a separate letter. I mean, I frankly don't know what Paul Chang's plans are for how the Policy Committee is going to communicate it's overall recommendations to ONC, but all of it is related in so way shape or form to the issues raised by the Meaningful Use and Certification rules. We just don't—some of our recommendations were not specifically asking for a modification or a clarification that can be done in those proposed rules.

Paul Egerman – Software Entrepreneur

It also appears to me that we made this recommendation about guidance before relating to transparency, and one would not necessarily expect that guidance recommendation to show itself in an NPRM. There's nothing wrong with this. I guess we're being redundant. I guess we liked our recommendation for guidance so much before we want to make it again.

Judy Faulkner – Epic Systems – Founder

This is Judy and I tend to agree with you. I think that we're really going a bit to the overprescribing of the—feel that we have to do this each time we have something like this. Also, I would worry that people

might interpret it as some legal document that the patients need to see them sign. Who know? You never know how that will be interpreted. And then—

Deven McGraw – Center for Democracy & Technology – Director

Judy, this is guidance that we've already approved, recommendations.

Judy Faulkner – Epic Systems – Founder

So why are we discussing it?

Deven McGraw – Center for Democracy & Technology – Director

Well, I'll tell you why it came up again. It came up again because there was some email discussion among the members of the—well, in the Standards Committee when they looked through the requirements for the portal a number of members of that committee were very concerned that patients would not necessarily fully understand the risks of taking information into their own hands and potentially sharing it with others. They were not aware that we had put forward a lot of very good guidance that we got through the Policy Committee. My recollection was unanimously endorsed. We're not overkilling anything arguably. We're just repointing to something that we already said that is directly relevant to a set of concerns that have been expressed about portals and the additional risk that might be introduced by making them more widely available and encourage a more robust

Judy Faulkner – Epic Systems – Founder

Well, then I kind of still go back to it; then why discuss it if, in fact, it has to be it has to be? If it doesn't have to be we discuss it.

Deven McGraw – Center for Democracy & Technology – Director

I don't understand what you just said, I'm sorry. If it has to be it has to be? I don't—

Judy Faulkner – Epic Systems – Founder

Well, I thought you were kind of saying we've already done it therefore it needs to be there so

Deven McGraw – Center for Democracy & Technology – Director

No. No. No. I guess I was reacting to what I thought you were saying that we don't—I thought that you were questioning the value of guidance to begin with and because that's what I thought I heard from you I was reminding you that we've already made that recommendation, and all I'm suggesting is that we point to it again.

Paul Egerman – Software Entrepreneur

So let's not get hung up on this issue because we already made a guidance recommendation, and I guess the proposal here is to point to the fact that we've already made a guidance recommendation. The guidance recommendation is not inconsistent with NPRM, and I guess there's no harm done if all we do is a few extra sentences and remind everyone that's what we did. Does that make sense?

Rebekah Rockwood – Markle Foundation – Manager, Health

Yeah. I think that makes sense.

Deven McGraw – Center for Democracy & Technology – Director

It does.

Paul Egerman – Software Entrepreneur

Okay. So I appreciate everybody's comments on this. I also want to get into one of the issue that's sort of like at the heart of a very difficult issue, which is EHR module. Although what we just finished I just want to point out this great progress. Some of these patient portal issues were troubling and we've gotten through a very difficult issue and very important issue. So EHR module is also a complicated issue, and to you want me to take us through this, Deven?

Deven McGraw – Center for Democracy & Technology – Director

Sure. Go ahead, Paul.

Paul Egerman – Software Entrepreneur

No. I'm sorry, do you want—?

Deven McGraw – Center for Democracy & Technology – Director

Oh, Okay. Yes.

Paul Egerman – Software Entrepreneur

Actually, I did not want to do it so I was hoping you would do it.

Deven McGraw – Center for Democracy & Technology – Director

No problem, I'm sorry. We have started to talk about this on a previous call so just quickly to remind everybody where we sit, the Stage 1 final certification requirements required EHR modules to be tested for all of the privacy and certification requirements. Although there were some circumstances under which they could be excused from that requirement, but the default was yes you have to unless you can demonstrate that it would be impracticable for you to do so. In the backup slides there is some further detail on the rational for which you could be excused from this criterion.

In Stage 2 they eliminate this requirement for EHR modules, and instead require this new concept of a Base EHR to be certified for all privacy and security requirements. On the next slide we actually have a slide that the Markle Foundation allowed us to use on what constitutes a Base EHR, and it's essentially all of the pieces that are required to be in place in order to meet the Meaningful Use requirements. You can satisfy it by either getting a complete EHR, or by purchasing a single EHR module, or a combination of modules as long as the combination has been certified to all of the relevant criteria below, and, again, it includes the privacy and security pieces of that.

So the question becomes whether this new concept of a Base EHR and the requirements that it be certified for privacy and security requirements, but not for other modules that are not part of the Base EHR but that a provider might purchase in order to meet—I actually can't say that I fully understand what these extra modules would do if they're not part of the base but they're additional products that are not necessarily—Joy, can you help me out?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yes. So the term that they're using as a Base EHR is what used to be called under Statute a qualified EHR so it's the essential components of an EHR that are similar across both ambulatory and in-patient. Then, there are other components of an EHR that are unique to each of those types of EHRs. So the base is the components that are necessary across both. Does that help any?

Deven McGraw – Center for Democracy & Technology – Director

Yeah. But I guess my question is whether somebody would need an EHR module to meet Meaningful Use that wasn't necessarily part of the base?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Things like Public Health reporting are not a part of the Base is it?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

I need to look at these criteria again to answer.

Judy Faulkner – Epic Systems – Founder

What about something like a cardiology module or an OB module or an ophthalmology module? They all deal with patient electronic health information, but they may be separate modules that an organization uses.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Or even emergency rooms too.

Paul Egerman – Software Entrepreneur

Something even more basic is maybe somebody produces a module that produces some of the quality report.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right, for ePrescribing.

Paul Egerman – Software Entrepreneur

Yeah. But that produces quality reports for you.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. You're right. The quality reporting one was the one that might differ very much by specialty.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

It does.

Paul Egerman – Software Entrepreneur

Yeah. So you have somebody that does quality reporting for, I don't know, oncology and so that might be an example of something that's not in the Base EHR, but might be an important part of Meaningful Use but some of these things may not apply to it. In other words, there's no patient authentication involved in that entire process. It's just somebody takes data from an EHR and does something with it and produces a report.

Deven McGraw – Center for Democracy & Technology – Director

Right. So then, just flipping back a slide because I want to re-iterate the point the Standards Committee had adopted a different recommendation to address the question of whether all EHR modules should be certified for all of the privacy and security criteria, and we've summarized it here in the slide. There are more details in your backup slide. And their recommendation was yes implement the criteria or demonstrate the capability to achieve those protections through being able to integrate with a module that does have it, or module or a Base or a complete EHR that does have those criteria in order to ensure that there would be an ability to sort of hook-in to some functionality that would be capable of providing some protection for the data.

Our options for how we comment on this—and this one we did get some feedback from Policy Committee members, both of whom are on the Tiger Team but not able to be on this call, about how important it is to make sure that the providers have sufficient technical functionality at their disposal to protect the data even if it's in a module. We could defer to the Standards Committee to address this because that was really the source for the privacy and security recommendation for certification for EHRs from Stage 1. Don't comment at all and assume that the obligation to comply with the HIPPA Security Rule is sufficient. Comment by endorsing Standards Committee approach, or comment by re-iterating our previous recommendation that the default approach be that EHR modules must meet all of the privacy and security criteria unless they can demonstrate that it would be impractical for them to do so, such as the patient authentication for measurement module that Paul just

Judy Faulkner – Epic Systems – Founder

This is Judy. May I just ask a question, some clarification because I'm not sure I understand this?

Deven McGraw – Center for Democracy & Technology – Director

Yeah. We may not either.

Judy Faulkner – Epic Systems – Founder

So let's say that a healthcare organization purchases an EHR but they want one module to be different, and let's say that module is the ED module, and maybe there are 100 ED modules available for them to purchase. How does that get certified? Does each vendor's ED module have to be tested with each EHR

base vendor? Does the healthcare organization have to do it by themselves? Do the vendors have to get together and do every combination? Maybe I'm missing something. I don't see this.

Paul Egerman – Software Entrepreneur

Judy, this is Paul. You asked like what I consider a great question. It's sort of like strikes at the heart of what this is all about because the Standards Committee, to understand what they're saying, they say you test it when it's integrated with the rest of the EHR, but it's really impractical. If you have an ED module you don't know what other EHR system it's going to be integrated with, and there's not standards for how that interfacing will occur. And so there's no way to test it against every combination.

Judy Faulkner – Epic Systems – Founder

And then, if you take that one further and you say, "Well, it's an ED module plus it's a cardiology module," and maybe there are 100 ED modules out there and 150 cardiology modules. You get into some pretty big combination numbers.

Paul Egerman – Software Entrepreneur

Well, that's right. And then, if you look at the example that I tried to give where some vendor has an EHR module that does something like produces a package of quality reports where there's really not the same sense of a user interaction with that module or even patient identification with that module. It just takes some data and produces reports. It's hard to figure out what you're going to test it for from a privacy and security standpoint. I don't know what that test is going to be and so I look at this and it's a thorny issue, and I don't know how to comment on it other than to say like no comment. In other words, you've got the compliance with the HIPPA Security Rule and that should suffice, and you do your best with that. I have a fear that to the extent you do something different you create a testing environment that just plain doesn't work in a lot of scenarios. That's hard to predict.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think the concern that I have, and we've interacted a little bit on this in the Standards workgroup, is that there doesn't seem to be a criterion that says a module needs to be able to interface with security services provided by the Base Module. So you could have, for example, the Base Module could start up a quality reporting module and that module could run as itself without any visibility on what individual users did within—the actions that they took within that module. I think how it fits, that interconnection between the module and the Base EHR security services is what I think that we need visibility for.

Paul Egerman – Software Entrepreneur

This is Paul responding. It's hard to know. You gave an example of a quality reporting system and if you have like an ED system or a cardiology—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It gives better—yeah, does a better—

Paul Egerman – Software Entrepreneur

Actually it may not be because they may exist like a standalone module. It may do its own independent security system for that departmental system and simply pass data to the EHR system. The patient is admitted from the emergency department to be an inpatient, and so it's hard to know what you test against. It's hard to say this is the rule for every module.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's a good example because that's what we really originally recommended was that the module either do its own security or assign security responsibility to another component—in this case it would be the Base EHR—and show how it interacts with that security provided by that external component. For example, if you had single sign on and the external component, the base system authenticated the user, passes the users authenticated identity to the module, is that module able then to take that identity and attribute the actions that it does to that identity and either record or use the external auditing to record the actions of the users. What is the linkage there?

If you really had this external module that did its own security then that's fine; it does its own security. It's not ideal by any means but you know that the securities still done and it would still need to be, presumably, assessed against—well, actually it wouldn't. In this case they say the EHR module doesn't have to be tested against the security so in your example where you had an ER module that did its own security that security would never be tested because that's what it said, "EHR modules don't have to be tested against the security."

Deven McGraw – Center for Democracy & Technology – Director

Yeah. This is Deven and I'm not exactly sure how to address this other than to relay a concern that at a minimum that providers who are purchasing a module that isn't part of a Base need, at a minimum, to understand that it's not tested for any privacy and security capabilities or the ability to be able to hook into any of them or use any of the ones that are present in the Base EHR, to use non-technical terms. For some modules it might be very important that the module has some basic security functionalities but the measurement module that's largely pulling and reporting aggregate data maybe less so.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

This is Wes. I just have a question. I'm sorry, it might have been said in the last few minutes, but they were mowing outside. I believe under Stage 1 if a site integrated a third party certified module with its EHR it had to be site certified.

Paul Egerman – Software Entrepreneur

No, not site certified.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. My understanding is that wasn't the case.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Not site certified, okay.

Paul Egerman – Software Entrepreneur

I mean, it could be site certified but it wasn't required. What would happen that was causing problems was if they purchase a complete EHR they had to—the vendor of the complete EHR had to re-certify itself for each module that was not included by the module that was purchased. And that meant each module of the complete EHR had to be tested for its own separate security, which drove some of the vendors completely crazy because they'd rather sell a complete EHR anyway, and now to have this extra obligation put on them just because somebody wasn't purchasing one part of their system seemed odd.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So it really boils down to the header originating modules, right. There are some modules that can actually operate standalone and operate as an EHR for limited scope, and those probably ought to be certified to the same level as a Base EHR, but it's really hard to nail that down with any specificity.

Judy Faulkner – Epic Systems – Founder

This is Judy. If you think about it in different ways it could be that by requiring this it really is a huge difficulty on the niche vendors because the push then is going to be that you don't use the niche vendor system because perhaps it has not been certified that way. I think it's going to make it really hard for those vendors.

Paul Egerman – Software Entrepreneur

Yeah. And what we want to do is we want a level playing field. We want to make it possible for niche vendors to succeed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And what you really want to encourage is for these niche vendors to actually use the security services of the Base EHR, and by just not certifying anything it doesn't even encourage that they use the Base EHR

security. It doesn't say anything. I think at the very minimum they should at least describe, define their interfaces with the Base EHR security services.

Paul Egerman – Software Entrepreneur

Well, that sounds good, Dixie, but that's not certification criteria. To me certification criteria are objectively testable. It should not be judgmental.

Judy Faulkner – Epic Systems – Founder

There's another interesting issue to it too, which is does it matter what interface engine they use because perhaps niche vendors product one works differently with one interface engine than another in respect to this and that gets into all sort of complicated combinations.

Rebekah Rockwood – Markle Foundation – Manager, Health

I have a question. Would it be possible for a vendor who made a module to get tested to the privacy and security criteria and to—?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yeah. That's the current requirement.

Rebekah Rockwood – Markle Foundation – Manager, Health

No. I know that. Under the proposed rule like let's say you just wanted to go above and beyond and show that you actually could meet those criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No. If you're an EHR module you don't get tested against it.

Paul Egerman – Software Entrepreneur

That's a good question though. But assuming each module then maybe you would want to get tested. Again, let's go back to the ED niche standard. Maybe they want to get tested to show that yeah they meet the criteria with it. Why couldn't they be?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, I think they'd have to—actually, if they said, "I'm an ED module and I'm a security module," they could, but they would have to declare themselves a security module within that. But they could do that.

Deven McGraw – Center for Democracy & Technology – Director

Well, I don't know that answers the question of whether one can voluntarily ask to be tested to meet criteria that you're not required to meet but that you'd like to demonstrate to potential purchasers that you can meet. I don't think you have to declare yourself a module in order to enjoy that. You might have to pay extra for it. I don't know how the certifying bodies are treating—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, it's also questionable, you know, if you wanted to—I'm going to check this because if you presented yourself as a security module what would you be tested against if the NPRM says, "Modules aren't tested against security"?

Deven McGraw – Center for Democracy & Technology – Director

Unless that's part of being a Base EHR then it would be.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yeah. You'd have to be certified as a base. Can you be a module for a Base EHR?

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Software Entrepreneur

So let's just do a check; where are we on this discussion? The way I hear this discussion; I'm not hearing anybody suggest anything different than no comment with the possible exception of whether module vendors can voluntarily get themselves certified. Is that what I'm hearing?

Judy Faulkner – Epic Systems – Founder

Paul, if they don't is it the Base EHR vendors obligation to certify every combination?

Deven McGraw – Center for Democracy & Technology – Director

No.

Paul Egerman – Software Entrepreneur

No.

Judy Faulkner – Epic Systems – Founder

Okay. So it's just kind of a voluntary thing that the niche vendors could do that so then the problem remains on the shoulders of the healthcare organization who has to make sure that everybody has done it.

Paul Egerman – Software Entrepreneur

Yeah. And the argument there could be when it comes to privacy and security that's where the obligation lies anyway because privacy is not a technical—it not something that you solve technically anyways. It's something you solve with a combination of technology and policies and procedures, and so that's what the organization has to make sure of, that the stuff works right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Security is technical.

Deven McGraw – Center for Democracy & Technology – Director

Well, but the security rule obligation is to protect all EPHI regardless of whether it's sitting in a module or it's sitting in a Base EHR or complete EHR will exist. It's really a matter of whether a provider can rely on certification to necessarily provide them with the tools that they need in order to comply with applicable security policy. And it sounds like they've got some basic tools that have been required in Stage 1 and will be present and tested in the Base EHR, but beyond that if they go the module approach and buy certain modules they will no longer, if the proposed rule approach takes effect, have a guarantee from a certification standpoint that the product that they're buying has tools that will help them comply with law. The legal obligation does not go away. It's whether you can rely on certification as your crutch to get you compliance, and it sounds like the answer may have to be no. You're going to have to do some work with the vendors when you're buying modules to make sure that you've got all the tools that you need.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Isn't that a requirement for meaningful use anyway to do that security evaluation?

Deven McGraw – Center for Democracy & Technology – Director

It's to do the risk assessment, right, but it's not tied 100% to compliance with all four corners of the security rule itself. That has its own sort of set of compliance tools, and, in fact, the proposed rules have actually been very clear that ONC doesn't consider certification to be a tool for enforcing compliance. It's also, the same for meaningful use, compliance with HIPAA.

Paul Egerman – Software Entrepreneur

Yeah. So what are we trying—we're looking for more certification here. I think we've got the fundamental issue that they have decided that the complications associated with testing modules for security outweigh the benefits when you look at the broad spectrum of things that might be modules.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's exactly right.

Paul Egerman – Software Entrepreneur

So it would seem to me what we're trying to come up with is possible responses to say what they said is okay. It makes sense to us as long as the module vendor, niche vendor can still get their module certified if they want to.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I don't—I mean, your argument for that is to say, "Though they feel difficulty in selling their products to actual eligible providers or hospitals because it can't be certified for security even though that eligible provider or hospital has to do a security risk assessment anyways." I honestly don't think that's a big factor.

Paul Egerman – Software Entrepreneur

Okay. So your solution is basically no comment on this.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, my solution would be to try to find some wording that looked at modules that walked and quacked like an EHR and so they ought to be secure like an EHR.

Deven McGraw – Center for Democracy & Technology – Director

And maybe the approach and comment is to raise concerns that EHR modules that walk like a duck and talk like a duck aren't necessarily going to be required to meet the same privacy and security requirements if they're outside of being a Base EHR, and that does concern us but we're hard pressed to believe that an approach that said that all EHR modules must be certified to all the criteria is the right answer either. I mean, there's a difference between not commenting at all and raising concerns with the approach, but I mean we always try to ideally offer a solution but it just sounds like we just really don't have one.

Judy Faulkner – Epic Systems – Founder

It is interesting—this is Judy—that the philosophies of some healthcare organizations have of best-of-breed is really going to be challenging for them to keep going with.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, you know, when I look at the Base EHR definition, the modules that we've been talking about, I think, which was said by Judy raising ED as an example, probably does meet the Base EHR definition.

Judy Faulkner – Epic Systems – Founder

I agree.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yeah. So in that case I guess the only question I have is whether it's possible to sell something that does meet the Base EHR definition of a module without having it be qualified by the Base EHR definition, be certified by the Base EHR definition. And I think there's a way to construct a coherent comment around that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

So what you're saying is if—referring to our earlier conversation—if I have an ER module, I think, but it also does security I should present it as a candidate for a Base EHR instead.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, you're talking about a marketing decision by a vendor. I'm talking—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No. No. Certification, how I want it certified. If I want the security certified, let's say, which is what we were talking about—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well who is I?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'm the vendor. I made it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yeah. So you're talking about a business decision that the vendor makes. I am skeptical that very many vendors will find it a business necessity to be certified on anything they don't have to. I don't think that—I wouldn't recommend to a client that they rely on certification in lieu of an evaluation of the product because I don't think certification is that strong under the best of circumstances. So to me the recommendation that we might make is that where a module includes the functions in the first five rules on the Markle slide it also must be certified for privacy and security. In other words, if it collects demographics, vital signs, med lists, allergy lists, does drug allergy interaction checks, provides computer ..., it does clinical quality measures, and does transitions of care then it needs to have the privacy and security certification.

Paul Egerman – Software Entrepreneur

And when you say those first five, it's all those five or any of the five?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I was thinking all of those five, although it's a reasonable question to say any of those five. It might leave out clinical quality measures, to be honest.

Paul Egerman – Software Entrepreneur

Yeah. As long as it does the first three.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Good enough.

Deven McGraw – Center for Democracy & Technology – Director

And four, the exchange of data.

Paul Egerman – Software Entrepreneur

That's five.

Deven McGraw – Center for Democracy & Technology – Director

Sorry, thank you.

Paul Egerman – Software Entrepreneur

Okay. So we've got sort of a conclusion. We'll accept this; however, if a module does many of the things that are put in here as a Base EHR—we're going to have to like word this a little bit—then it should be—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

If a module being certified includes most of the Base EHR capabilities listed in the four that we've identified then it should be certified for privacy and security.

Paul Egerman – Software Entrepreneur

Okay. I think that's a good resolution. Any disagreement?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No. That sounds really good. I am concerned too with the module that is a separate module but doesn't use any of the base security. I don't know what the answer is. I agree with Deven. I don't know what the answer is but I think it's an issue.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think that's where ONC has decided to throw in the towel, and I think that unless we have any way to believe that there is a solution to it we're better off not commenting.

Paul Egerman – Software Entrepreneur

So we've completed the EHR modules. There are five areas that we had to discuss, and we've discussed patient portals and EHR modules, which are two of the hardest. We have just like three minutes left, and I don't know, do you want to quickly—

Deven McGraw – Center for Democracy & Technology – Director

I think we might be able to get through ePrescribing.

Paul Egerman – Software Entrepreneur

If we did that would be like unbelievably great, but let's talk fast. See if we can do it because we've got like three minutes.

Deven McGraw – Center for Democracy & Technology – Director

We've got three minutes. So here's where we have recommended that the certified EHR technology have the capability to support the two factor authentication as required by the DEA interim final rules.

However—sorry this is not on the slide—we recommended that this be in place by Stage 3, and ONC declined to propose for Stage 2 noting potential conflicts with state law and challenges with widespread availability of products that include the functionality to support the DEA requirements. Paul and I also got some feedback from the Policy Committee that many states have particular requirements with respect to prescribing controlled substances that their providers would need to follow outside of using a certified EHR to do it. In addition, I've had some subsequent conversations with the ONC where they reminded me that, in fact, there is a DEA certification process that one of the EHR certifiers has been deputized to run.

ONC did also request comment on the availability point.

So here do we reassert our recommendation for either Stage 2 or Stage 3 or do we do what ONC seems to have done, which is to rely on these other efforts including market demand at least for Stage 2, and address the need to look at uptake prior to Stage 3 and consider it in Stage 3 if the availability is still not widespread?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But Stage 3 would be consistent with our prior recommendation.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. It would be.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yeah. As I recall ONC also recommended the concern about multiple agencies regulating the same thing, which, god forbid—

Deven McGraw – Center for Democracy & Technology – Director

That never happens, Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No. No, never. So I would say that given that it's already—it's going to come up again with the Policy Committee for Stage 3 so I—same thing no comment would be what—to save the people in ONC at least a half an hour an Christmas Eve going for a comment.

Paul Egerman – Software Entrepreneur

Is there any disagreement?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No.

Deven McGraw – Center for Democracy & Technology – Director

I think we did that in two minutes. Sorry, now it's three.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Okay. You all do realize that ONC stands for the 'office of no Christmas'.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yeah. I was thinking this is probably closer to the office of no Memorial Day but I can't think of the acronym for that.

Paul Egerman – Software Entrepreneur

So this is great progress. We got through three important issues; the patient portal, the whole issue of the module, and ePrescribing. We still have left two more issues, which are the digital certificates and patient matches, which we'll do at our next meeting, but let's first see if there's any public comments.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Okay. Operator, would you open the lines please.

Operator

We do not have any comments at this time.

Paul Egerman – Software Entrepreneur

Terrific. So thank you very much. It seems like we made a lot of progress. Our next meeting is April 23rd. Is that right Deven?

Deven McGraw – Center for Democracy & Technology – Director

Yes, that is correct.

Paul Egerman – Software Entrepreneur

And what time is it on April 23rd?

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

It's at 2:00; 2:00 to 3:00 so you only have an hour. You'll have to go back to talking fast.

Paul Egerman – Software Entrepreneur

Okay we have an hour, and we have two topics and perhaps a fourth. That meeting we can also write a draft of what we've done so far; the format of what our letter is going to be to the Policy Committee so people will have a chance to look at it. But terrific progress; we're just about there.

Deven McGraw – Center for Democracy & Technology – Director

I agree, Paul. That's great; great idea. Thanks everybody.

Public Comment Received During the Meeting

1. A vendor may present an EHR module for certification that is both part of a complete EHR and may be able to stand alone, and shares in the security model of the complete EHR - the issue with Stage 1 certification is that a vendor would have to certify the module for security capabilities previously inspected.
2. Some guidance on how to apply the concept of a base EHR needs to be established in this case so a vendor cannot present for modular EHR certification something not previously inspected for privacy and security
3. But at the same time, does not have to be inspected again and again for the same security capabilities if it has (the case of an EHR module being integrated with a complete EHR)