

Privacy & Security Tiger Team
Draft Transcript
March 28, 2012

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Good afternoon 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 and Security Tiger Team. It is a public call and there will be an opportunity at the end of the call for the public to make comments and I would ask the members to identify themselves when speaking. I'll begin by taking the roll. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Paul Egerman?

Paul Egerman – Businessman/Entrepreneur

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Dixie Baker?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I'm here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Christine Bechtel?

Alice Leiter – National Partnership for Women & Families

This is Alice Leiter.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

In for Christine? Rachel Block? Dan Callahan?

Deven McGraw – Center for Democracy & Technology – Director

You have an old list, Mary Jo.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Really?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, Rachel has not been on the Tiger Team for about a year.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Okay, that's good to know. I will certainly make note of that.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

How about Dan Callahan?

Daniel Callahan, Ph.D – The Hastings Center

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Neil Calman? Carol Diamond?

Rebekah Rockwood – Markle Foundation

Rebekah Rockwood for Carol.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Judy Faulkner? Leslie Francis?

Leslie Francis – National Committee on Vital & Health Statistics

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Gayle Harrell? John Houston?

John Houston – University of Pittsburgh Medical Center – NCVHS

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

David Lansky? David McCallie?

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

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Verne Rinker? Wes Rishel? Micky Tripathi?

Micky Tripathi – Massachusetts eHealth Collaborative

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Latanya Sweeney? And could I ask staff from ONC and any other agency to identify themselves at this time please?

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Joy Pritts.

MacKenzie Robertson – Office of the National Coordinator

MacKenzie Robertson, ONC.

Verne Rinker – Office for Civil Rights

Verne Rinker, I was here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Good, okay, thank you, back to you Deven.

Deven McGraw – Center for Democracy & Technology – Director

All right, great, thank you very much Mary Jo.

Judy Faulkner – EPIC Systems Corporation

Judy Faulkner has joined too.

Deven McGraw – Center for Democracy & Technology – Director

Oh, great, thanks, Judy.

Judy Faulkner – EPIC Systems Corporation

Sure.

Deven McGraw – Center for Democracy & Technology – Director

Anybody else who missed roll call want to chime in? All right, great, we have a short meeting today, only an hour and slightly less than that because we always leave room at the end for public comment and we welcome the members of the public who are listening in on the telephone call. Let's just quickly review the agenda here.

Opening remarks we are right in the middle of. What we're trying to do is to continue to make progress in taking a look at the recommendations that we have made on privacy and security that were relevant to the Stage 2 proposed Meaningful Use and certification rules looking at how those proposed rules came out and considering whether there are additional recommendations that we want to make during the comment period for those rulemakings, which is up in early May. So, we will get as far as we can on this call, continuing the discussion that we began on our last call and at the Policy Committee meeting in April, which is next week Paul and I will discuss the progress that we've made on recommendations so far and also tee up the other issues that we're continuing to consider with the hope of wrapping up the discussion in its entirety by the May Policy Committee call. Remember that what we decide as a Tiger Team still must be endorsed by the Policy Committee before it can be forwarded onto ONC. Paul, do you have anything to add before we jump in?

Paul Egerman – Businessman/Entrepreneur

No, I just want to comment that after the last Tiger Team call one observation that we made that is very important is that we need to resist the temptation to sort of rediscuss issues that we've already made decisions about, the way we're suggesting that we go through this entire process is to see what is the variance, what is the difference between what is in the NPRM versus what we already recommended, that's probably the best place for us to focus at least to get started.

Deven McGraw – Center for Democracy & Technology – Director

Yes, thank you, Paul.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

And this is Joy, I'd like to throw in just another gentle reminder too, which is there is this concept of logical outgrowth. So, whatever is in the final NPRM must have been somehow connected to what is in the NPRM.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

It has to be logically connected, so if it wasn't at all discussed or raised or even touched in some manner in the NPRM; it will be extremely difficult to get it incorporated into the final rule.

Deven McGraw – Center for Democracy & Technology – Director

Another very good point, so helping us to focus on, you know, not to redo the recommendations we've already done, but to focus on what of those recommendations got adopted, and whether there's more that we can say, and not to try to introduce completely new items that are not logically an outgrowth of what was in the proposed rule. Very, very good points.

Micky Tripathi – Massachusetts eHealth Collaborative

This is Micky, just one quick...

Deven McGraw – Center for Democracy & Technology – Director

Micky, we can barely hear you.

Micky Tripathi – Massachusetts eHealth Collaborative

Oh, sorry, is that better?

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Micky Tripathi – Massachusetts eHealth Collaborative

Just a quick clarifying question, Joy on that, if somewhere in the preamble or elsewhere in the NPRM it says we considered this because it was a recommendation from the Policy Committee or Standards Committee but we chose not to include it, is that fair game?

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

In particular where comments are requested on that piece that's fair game.

Micky Tripathi – Massachusetts eHealth Collaborative

Okay, thanks.

Deven McGraw – Center for Democracy & Technology – Director

All right, great. But before we launch into a discussion of the rule I want to turn the microphone over to Joy to give you all an update on some guidance that The Office of the National Coordinator put out recently that's relevant to some recommendations that the Tiger Team and the Policy Committee have made in the past. So, Joy, is this is a good time?

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Sure. I just want you all to know that your hard work has come to fruition. As you all remember the Tiger Team submitted a number of recommendations to us quite a while ago on a number of privacy topics including consent, transparency, patient access, primarily in the health information exchange context, and those recommendations were considered by HHS in a very lengthy process shall we say, and the result of that has been that our office has issued a program information notice to our state HIE program grantees last week on the 22nd, which incorporates a lot of your recommendations. So, we would like to thank you for all of your work that you did and to let you know that actually we do listen and that your efforts actually do produce results.

Deven McGraw – Center for Democracy & Technology – Director

Well, that's much appreciated, Joy and I think if we were not as pressed for time with comments on these rulemakings, as we were, we would probably would spend some more time on this call detailing exactly what's in that notice, but at least at this stage, we've included the link for everybody so you can take a

look at it. It's not actually that long, but I think a lot of what's in there will look very familiar to those of you who remember, particularly the summer of 2010. When we spent a lot of time together as an initial Tiger Team and came up with some recommendations on fair information practices and consent. So, I know personally I was quite pleased. So, you should take a look.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

And we appreciate your patience.

Paul Egerman – Businessman/Entrepreneur

Well, that's worthy of a victory lap and a virtual fist pump, because that's a hard topic. So, thank you, Joy for that update.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, very good. Anybody have any questions for Joy? Ideally, not to the details of the program notice, but to the sort of general discussion that we just had before we move on?

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

You know what Deven; it is posted on the Internet. So, maybe we can have somebody send a link out to people if they would like.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, it should be on the slides, maybe not so easy for people to click on, but there is the URL.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Okay, great.

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. So, again today we're going to try to move through as many of the issues that we began to tee up on the last call. In general the recommendations that we have made as a Tiger Team and Policy Committee kind of fall into three categories really, fully adopted which as indicated in the e-mail that we sent to you all, we intend not to discuss on this call or any subsequent calls unless we get some indication from one of you that we need to discuss it.

Then there's the category of not sure, which is we are not entirely sure whether the recommendation was adopted because it wasn't exactly in the form that we proposed it, but may nevertheless still have been honored through other mechanisms and that is where we need some technical expertise and we're always thankful we have it here on the Tiger Team with some of the Standards Committee members.

And then the third category is well it just wasn't adopted at all and so we're really going to spend our time in the last two categories and here's a list of those that were fully adopted, the security risk assessment, including encryption of data at rest, most of what we said about amendments, although it doesn't include the issue of the capability of transmitting amendments, which we began to discuss on our last call and we're going to continue at the beginning of this call. And then the recommendation on a patient accessible log for the patient portal functionality, all of that was included in the proposed Stage 2 rules.

What's less clear to us, at least at first blush was our recommendations on data provenance for the portals, the recommendations we made on standard formats for demographic data fields, for improved patient matching purposes, the use of digital certificates. And then in the non-adopted category is the issue of transmitting capabilities to transmit amendments, secure download authentication and programmatic attacks for patient portals, previous recommendations that were made by the Privacy and Security Working Group that preceded the Tiger Team on EHR modules, ePrescribing with controlled substance, digital certificates, testing. The use of those digital certificates and then again much of what

we said on patient matching on address normalization and testing of the demographic formats. So, that's just a sort of global summary.

And with that I think we're going to launch into amendments and focusing really only on the transmission issue, because the recommendations we made about the ability to amend, to make amendments and to append data were adopted in the certification rule in terms of making sure that the EHR technology has the capability for providers to make the amendments and appending patient data in ways that they are required to do under the HIPAA Privacy Rule. So, now, I'm again trying to save time, so forgive me, I just went back and forth on slides, which is not so good. So, again, what we have said and this is important, because I think we had a lot of discussion on our last call about amendments that wasn't necessarily related to the actual recommendation that we made. We said that certified EHR technology should have the capability to support amendments, including a provider's ability to comply with HIPAA. So, that means making amendments to patient's health information in a manner that is consistent with the entities obligations with respect to the legal medical record and then being able to append information from the patient and any rebuttal from the entity regarding the data. This is all consistent with HIPAA.

What's in the proposed certification rule, is that certified complete EHRs and modules must have the capability to enable a user to electronically amend the patient's health record to replace information in a way that preserves the original and to be able to append patients supplied information in either free text or scanned format directly to a patient's health record or by embedding an electronic link, and then to be able to enable a user to electronically append a response to patient supplied information in the event that there is a rebuttal. So, that's the indication that our recommendations about amendments with respect to the making of amendments in the EHR by the provider who is the steward of that EHR.

Now, we also noted on our last call that HHS specifically requested comments on whether the EHR technology should be required to be capable of appending patient supplied information in both free text and scanned format or really only one of these methods in order to be certified to the proposed certification criteria, and tentatively at our last call we said, one we should praise ONC for adopting the recommendations that we made on amendments and we do think that the technology should be required to be able to both append the information in both free text and scanned format and we allowed our technologists on the call some time to check with their teams to see if that would be at all problematic and so that would be directly in response to a comment.

Now here's the transmission part that we got a little hung up on in our last call and that I'm hoping we can deal with quickly on this call. We made a recommendation that certified EHR technology should have the ability by Stage 3 to transmit amendments, updates or appended information to other providers to whom the data in question has been previously transmitted. This was a recommendation that was narrow in scope and intended really to enable providers to transmit amendments, updates, or appended information to other providers when they are required to do so by law, or when they desire to do so on their own accord. We did not make a recommendation for example that said the technology has to have the capability to identify recipients with whom the information was shared. Nor did we necessarily have a policy recommendation about who should be required to receive amended information.

Our recommendation on the issue of transmission of amendments was limited strictly to the capability to transmit amendments when providers desire to send them either because they're required to do so by law or they want to. We did not opine on the policy issues of who should receive amendments and we really got really hung up on our last call about the issue of identifying who should receive amendments, etcetera, etcetera.

Paul Egerman – Businessman/Entrepreneur

And Deven this is Paul.

Deven McGraw – Center for Democracy & Technology – Director

Yeah?

Paul Egerman – Businessman/Entrepreneur

To be clear or to repeat we also said this transmission capability had to be present by Stage 3.

Deven McGraw – Center for Democracy & Technology – Director

That's right, thank you Paul.

Paul Egerman – Businessman/Entrepreneur

By Stage 3, which is underlined on the screen. So, in some sense that's not inconsistent with what's in the NPRM, in other words, you know, the NPRM doesn't do anything for Stage 2, but we didn't ask them to do anything on transmission in Stage 2.

Deven McGraw – Center for Democracy & Technology – Director

Right, but I guess, you know, so one thing though that we have teed up, as you'll see is whether it's appropriate to signal in this Stage 2 rule that that capability should be there for Stage 3. And this time, to help us with our discussion, Paul and I, and Joy and the folks from MITRE pulled together some strawman, strawdog, as Micky likes to call them, potential comments for your discussion and that would be, I'm on slide 11, you know, obviously we can say nothing about this because really our recommendation was for Stage 3 and not for Stage 2 or we have the option of commenting that it's important that the technology have the capability to allow amendments and appended information to be propagated forward and that ONC should at least in the final rule signal the intent to require this capability in Stage 3.

And, I think, I'm just going to take a peek at the next slide to see if that's what...yeah those were the options that we put on the table. Obviously the discussion doesn't have to be limited to those options, but we wanted to at least have a couple teed up for your consideration.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Deven, this is Dixie, is it normal practice to, you know, warn them in the preamble that this is coming to Stage 3? I know that sometimes it's done, but is it a, you know, a standard practice to do that?

Deven McGraw – Center for Democracy & Technology – Director

I mean, I certainly don't think that the rules to the extent that they speculate or state with some specificity that something will be required in Stage 3. I don't think that's universally adopted for every potential Stage 3 measure, but we certainly have lots of examples where, you know, if ONC was certain or fairly certain that by Stage 3 they wanted to encourage a certain behavior, they've indicated that. In the Meaningful Use rule for example, in both Stage 1 and in Stage 2 it has said we anticipate a Meaningful Use objective in Stage 3 that will involve the acceptance by providers of patient generated data.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

So, it's not unusual, I think it's not always used. Other comments? You know, and here's another thing I want to raise, I was wondering whether the transport, the fact that we have transport standards and the requirement to transport a consolidated CDA is that a vehicle that can be used for amendment purposes or am I mixing apples and oranges?

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

Deven, this is David.

Deven McGraw – Center for Democracy & Technology – Director

Yes, David.

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

I think, you know, on the surface, it's hard to argue with the spirit of what this means. I think that the challenge will be in figuring out how one would test for it and what the details are. So, just for example,

you know, using Direct or XDR capabilities that will be a part of Stage 2, any provider could resend something that he has already sent that has changed and that doesn't require any technical advance beyond what we have today. The question is what will the receiver do with it, will they merely add it to the existing database or will they recognize that it is in fact an update to something that they've seen before, keep track of them, and appropriately merged them so that the original is preserved and the new changes are now.

Paul Egerman – Businessman/Entrepreneur

David that's a great question, but it's actually one we don't have to address right now.

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

Okay, so I'm just saying because that is what it will hinge on.

Paul Egerman – Businessman/Entrepreneur

Yeah, because again, we're really trying to decide whether or not we want to signal something for Stage 3.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Businessman/Entrepreneur

And, so I guess your point is if you signal that for Stage 3 you might want to signal something more, you know, because one would think that if you're going to transmit some change the receiver has to somehow, you know, absorb the change. It doesn't make sense to only have a transmission without a reception capability perhaps, I don't know, maybe it does, but the real question is do we want to ask, I guess, I don't know if it's CMS or...?

Deven McGraw – Center for Democracy & Technology – Director

It would be ONC for the certification requirement.

Paul Egerman – Businessman/Entrepreneur

ONC to signal this, if that's important to do, one could argue it's not important to do because in fact, just by writing a letter we're signaling it and we seem to have a good track record and vendors and everybody are paying attention to what we're saying. So, you could argue that that's adequate or you could argue that gee it doesn't cost much to signal it and we should go ahead and recommend that.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

This is Dixie. The Privacy and Security Standards Workgroup, one of our recommendations on the appending piece that is in the proposed rule is to delete everything after appended patient supplied information because we felt that it shouldn't be limited to free text or scanned, in fact we even left open the option that, you know, a patient could in fact submit a consolidated CDA of their own or perhaps from the PHR or something like that. So, we recommended not constraining the way that the patient supplied information was appended and I think that's a good recommendation, and if they take that recommendation, I think signaling that downstream they may be required to submit it might influence how they would implement the appending.

For example, you know, it currently could be a link. Well, you know, transmitting a link is something different from transmitting a revised CCDA. So, I think that there could be some benefit there.

Paul Egerman – Businessman/Entrepreneur

So you think there's value in signaling it and so as a result we should suggest to ONC?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Yes, does anybody have any objection to that? Again, I don't think we have to work out the details. I think we just have to reiterate that this really should be done by Stage 3.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

And that would encourage people to bring up issues as well.

Deven McGraw – Center for Democracy & Technology – Director

Right, when there's time to do so, as opposed to, you know, 2 years before we want to implement it.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes.

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

Yeah, this is David; I certainly have no objection to signaling it. I think it's a good sound system design to be able to do this. It just does push the standards that we have a little bit. So, work might be required.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I suspect it will.

Leslie Francis – National Committee on Vital & Health Statistics

This is Leslie. It's also a tremendously important thing for patients.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Paul Egerman – Businessman/Entrepreneur

Okay, so it sounds like no one has spoken against it.

Deven McGraw – Center for Democracy & Technology – Director

Yes, that sounds good.

Paul Egerman – Businessman/Entrepreneur

I think we have a recommendation.

Deven McGraw – Center for Democracy & Technology – Director

A consensus.

Paul Egerman – Businessman/Entrepreneur

Yes.

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. All right, the next several slides in the deck that we sent you have to do with recommendations that we made relevant to both Meaningful Use as well as certification criteria and on guidance that we urged ONC to issue related to the patient view, download and the transmit capability. That is in the proposed rules for Stage 2; we called them patient portals when we dealt with them. There were a number of issues that I was initially planning to dive into on this call, but I know that the Standards Committee, based on some e-mails back and forth Paul and I have had with members of the Standards Committee that a number of members of the Standards Committee have raised a number of issues too.

And since this sort of set of issues around whether we have the right set of policies and technical capabilities in place or will have them in place with both what's been proposed in the rules and what we said with respect to our recommendation on guidance that would be provided to patients, it doesn't feel quite right for us to try to dive in on it on this call and it feels like it might benefit from a little work off-line jointly with some of the standards members, and Paul and me and anyone else on the Tiger Team who is interested, so that we can maximize use of Tiger Team time by presenting some initial conclusions for your consideration that benefit both from the standards discussions as well as policy discussions.

Does that make sense to everyone, that would essentially mean that we would tee this up, we would hold this and not try to deal with it for the April Policy Committee, but work to resolve it for the May Policy Committee and do some work off-line to develop the right set of strawdog options. What do folks think about that?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I think this is, this is Dixie, this topic is raising a lot of questions within the Privacy and Security Standards Workgroup. So, I do think that this topic can benefit from some discussion that involves both of those groups, yes.

Deven McGraw – Center for Democracy & Technology – Director

Okay. And assuming that means you're also willing to help us out with this?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes, yes.

Deven McGraw – Center for Democracy & Technology – Director

All right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

And I might suggest a couple of others who raised issues on this exact topic at the standards meeting on Tuesday.

Deven McGraw – Center for Democracy & Technology – Director

I think that would be great. Does anybody have an objection about that? And does anybody want to also volunteer their time.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

David does.

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

Yeah, David's arm is being twisted.

Rebekah Rockwood – Markle Foundation

This is Rebekah, I think it sounds like a good idea and I'd also volunteer.

Deven McGraw – Center for Democracy & Technology – Director

Okay, great, thank you Rebekah.

Deven McGraw – Center for Democracy & Technology – Director

All right, well Paul gets roped in whether he wants to or not and I am committed to figuring this out. So, we will off-line discuss a process for trying to tee up some potential policies and standards recommendations for both working groups to consider.

Paul Egerman – Businessman/Entrepreneur

That is fine with me, it's just a bit of a mixed metaphor that David got his arm twisted and I got roped in but that's okay.

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

We can virtual fist pump no matter what.

Paul Egerman – Businessman/Entrepreneur

Right, we'll figure something out.

Deven McGraw – Center for Democracy & Technology – Director

All right, that sounds good. So, that allows us to move to pretend as though we've resolved a lot of things and move all the way to EHR modules. Look at that. Look how much progress we made or we will make. So, this was really pre-Tiger Team work. It was done by the larger Privacy and Security Working Group of the Policy Committee. A number of you who were on the Tiger Team were part of that Working Group, but many of you were not, but nevertheless, since we are not using that Workgroup anymore and are using the Tiger Team now for privacy and security issues that come before the Policy Committee this is where this issue lands.

What the Health IT Policy Committee had recommended and this was really back in Stage 1, the Policy Committee strongly endorsed a default rule that all EHR modules must meet all of the privacy and security certification criteria. But the Standards Committee took a slightly different direction for this, which is completely within their purview and responding more to some of the concerns that some of the modular vendors had raised about, and maybe even the complete EHR vendors had raised, about this requirement and essentially what they said, and I'm only going to read this verbatim because it comes right out of the proposed rule and I don't want to misstate it, which is to enable the certification process to more effectively address security integration the Standards Committee Privacy and Security Workgroup recommends that the ONC and NIST consider modifying the certification process so that each privacy and security certification criterion is treated as addressable. To meet the criterion each complete EHR or module submitted for certification would need to either implement the required security functionality within the complete EHR or the module being submitted for certification or assign the function to a third-party security component or service and demonstrate how the certified EHR product integrated with its third-party components and services meets the criterion.

So what happened in the proposed rule? Here's what the certification notice of proposed rulemaking says, they proposed not to apply the privacy and security certification requirement for certifying EHR modules and they site stakeholder feedback particularly from the EHR technology developers that identified that this regulatory requirement is causing unnecessary burden in both effort and cost. So, what they stated is that based on the proposal that eligible professionals, eligible hospitals, and critical access hospitals must have a base EHR to meet our proposed definition of certified EHR technology that would apply beginning in 2014, we believe we can be responsive to stakeholder feedback with our proposal to not apply the privacy and security certification requirements to modules, while still requiring an equivalent or higher level of privacy and security capabilities to be part of certified EHR technology.

So, the base EHR, whether that's part of a complete EHR that is submitted for certification or a collection of modules, I interpret this to mean that the base EHR would have to demonstrate that the privacy and security certification requirements are met, but that outside of the base EHR the modules would not be required to meet or be tested for any of the privacy and security functions. That's the way I interpret it, I want to make sure if that is how others Dixie, David, others on the Tiger Team who have been paying some attention to this, if you interpret it that way as well?

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

This is David. I think that's the right interpretation. I believe the thought is that the security is typically a security and privacy issue, particularly the security side of it, are typically addressed at system-level rather than inside specific modules and that it was difficult to figure out how to test broad security if each module had to do something on its own when in fact system-level testing is more appropriate. I'm not sure how it translates to practice, but that was the spirit.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So, how did they certify a base EHR? I know how they certify a complete EHR, but I know that the base EHR is brand-new for this next, page 2, right?

Deven McGraw – Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But they certify base EHRs as well, right?

Deven McGraw – Center for Democracy & Technology – Director

Yes, well so you have to have a base EHR and then whether or not you pick up certain models outside the base EHR depends on whether you need that particular functionality in order for you to meet Meaningful Use.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

That's right, I remember, I remember the diagram, right that Steve presented and all, okay, now yes, yes. You know, the problem with this is that the way the Privacy and Security Workgroup recommended it; it would require that every module at least demonstrate that they could call a security service, right? And they the capability to be integrated with a security architecture.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I don't see that, this may not do that. You could have an EHR module that could not be integrated as part of a security architecture.

Paul Egerman – Businessman/Entrepreneur

Yeah, so this is Paul, and let me make a comment. See, I didn't read this section so I don't know what it actually says, but I can tell you what I think it should say, I don't know if it says it or not, but it should say that if a vendor submits a complete EHR for certification and it passes for certification then if a user, if an eligible hospital, eligible provider purchases that complete EHR, but chooses not to use one module, for example they choose not to use like an emergency department module and to get an emergency department module from somebody else. What the system should say is well that certified EHR is now a base EHR and its collection of modules do not need to be retested for security. But, the new thing that was not part of the complete EHR somehow does have to be tested for security and privacy. And my example of that would be the ED system.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

You know, that exact example was brought up at the Standards Committee when Steve Posnack presented to us and he said that they chose not to really address that problem this time around.

Paul Egerman – Businessman/Entrepreneur

Was that in Stage 2?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, it wasn't addressed. Go ahead, Rebekah.

Rebekah Rockwood – Markle Foundation

Oh, I mean, I think it's also important to do some...remember some of the discussions that happened around Stage 1 and the emphasis the certification program placed on certifying technology before the implementation stage. And I think once you tried to certify after there are different configurations and after people have implemented in different ways, it becomes much more difficult logistically and might create a situation that adds even more complexity.

Deven McGraw – Center for Democracy & Technology – Director

I think I am we're Dixie is, which is that I'm not convinced and I'm just going to move the slide to what we said for comment options. What worries me about what's been proposed is that there isn't any requirement to make sure that any module that is collecting PHI can connect into or independently has the capability that would be necessary to protect that data from a security standpoint. Is it enough to just say well providers do have security rule obligations for that data regardless of where it's sitting in a

module that has functionality or not, but to me then that means that the providers that are using modules that cannot connect into privacy and security functionalities that are present in another module or in the base EHR, will sort of be left holding the bag because they won't have any technology solutions to deploy to support their compliance with obligations to keep the data secure and to have technical physical and administrative safeguards.

So, I mean, I'm not the technical expert here, but my concern all along has been how do you know that the data in any module, that there's the capability to protect it if it's not either required to be independently tested to have that criteria or it's not required to show how it connects in. I'm sort of on the side of where you guys came out on the Standards Committee on this one; it seems to make sense to me.

Paul Egerman – Businessman/Entrepreneur

I think there's a solution to this and perhaps a disadvantage by not having gone through the text, it could be text is really trying to do this but I like the concept of the baseline EHR. To me the baseline is really a complete EHR minus a few of its modules, one or more of its modules, and so my view is if that's the definition of a baseline EHR then the modules within that do not need to be tested for privacy and security because they were already tested as a whole when the complete EHR was tested.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But you can certify a module outside the context of a base.

Paul Egerman – Businessman/Entrepreneur

Oh, I understand, so what I'm trying to say is if you define a base as simply a complete EHR minus one or more of its modules, I'm saying that does not need to be recertified for each individual module, because that would be burdensome.

Deven McGraw – Center for Democracy & Technology – Director

Well, yeah, but I don't...

Paul Egerman – Businessman/Entrepreneur

Burdensome and not likely to come up with any result. And so I see that as like almost like a division. So, the concept of the complete EHR and the baseline EHR being like a subset of the complete EHR that make sense that you don't need to test the modules for that. On the other side, if you buy a module separately, I can use an example, like an emergency department module, then it should be tested. You know, it's a single module that is not part of the complete or the EHR then it needs to be certified and tested for privacy and security.

Rebekah Rockwood – Markle Foundation

It would be helpful to understand, I don't know if anyone from ONC is on the call, but exactly what can be used to comprise a base EHR.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I have it in front of me; I can read it to you, if you like?

Rebekah Rockwood – Markle Foundation

Oh, yeah, my understanding is that it could be either, you know, one product or it could be a combination of multiple modules and that they wouldn't actually have to be tested, you know, they wouldn't have to be testified and certified together.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

It can be, but the point, this is Dixie; the point is a base EHR does have to have the capability to protect confidentiality, integrity and availability, right? But, the point is, if you have a base EHR and you have a module that you pass an identity to the module and the module doesn't do anything with it, you've got all the actions within that module that would not be auditable, you know, there has to be some linkage between a module and the security service architecture whatever it happens to be, whether it be an

enterprise-wide security service architecture or whether it be this base EHR, whatever it is there's got to be some way to link the actions that happen within that module with the overall security protection.

Paul Egerman – Businessman/Entrepreneur

Yeah, and Dixie, this is Paul, I'm agreeing as it relates to the module. I'm just saying that you have to define this thing called the baseline and within the base EHR you don't have to test every single module that is in the base.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, right.

Paul Egerman – Businessman/Entrepreneur

If it is part of a complete system.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

True, that's not what we're discussing though, you know, we're discussing and what we made our recommendation about is how do you certify a module? We're not really discussing how do you certify a base, it's how do you certify an individual module and we recommended that, no, you know, previously every module had to be certified against all the security criteria.

Paul Egerman – Businessman/Entrepreneur

Right, it becomes, Dixie an important issue because in Stage 1 we didn't have a definition of a base EHR. So, it was either a complete EHR or it was a bunch of modules together and the problem there is how vendors, who are vendors of complete EHR systems, get certified, because they do not necessarily want to have to certify every one of their modules individually.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right.

Paul Egerman – Businessman/Entrepreneur

And also certify them as a whole.

Judy Faulkner – EPIC Systems Corporation

This is Judy, yeah, I'm sorry, go ahead.

Paul Egerman – Businessman/Entrepreneur

Well, they don't want to do that so the idea of defining a baseline.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, I agree, that's a great idea.

Paul Egerman – Businessman/Entrepreneur

So the baseline is good and so that sort of say that's no longer a collection of modules that's the baseline and it does not need to be certified.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, but if I submit it as a module, I submit, I mean you can still in the topic is, how do you certify an individual module that is not certified with a base, it's certified all by itself as an EHR module.

Paul Egerman – Businessman/Entrepreneur

Right, now Judy was trying to say something.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, go ahead Judy, sorry about that.

Judy Faulkner – EPIC Systems Corporation

There are a couple of things in here. I think even if you have a complete EHR, almost all of them are still going to interface to something. There's just too many things out there that interfacing is done to regardless of whether they have a complete EHR or not. So, I don't think it differentiates a complete EHR and a base EHR that much, because they're still interfaces.

Then when you get into the base or complete EHR, which is interfacing out, my memory of our HIT Policy Committee meeting is that we don't have power over say the lab module to make it do or not do various things. When it comes back to, the data comes back to the complete or baseline EHR, whatever you want to call it, because I think they're reasonably synonymous, that it's still in its protected, I would think, data structures. So the danger is not the EHR itself, because that's going to still have its privacy, it's going to be in those modules that we don't have much of a say over at all and that is where the concern is.

Now, keep in mind there is another thing too. Some of the complete EHR vendors also will sell modules. So, it could be that they are selling their ED module as a standalone.

Paul Egerman – Businessman/Entrepreneur

That's correct.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Businessman/Entrepreneur

In which case it should be certified.

Deven McGraw – Center for Democracy & Technology – Director

I think there are some factual questions that I would like to get resolved before I would vote on this and one would be I want a more clear understanding of the difference between a base EHR and a complete EHR, because complete EHRs are presented for certification as a package. I didn't have the impression from reading the rule that base EHRs were required to do so. Every EP, EH and CAH has to have a base EHR, but if the base EHR isn't presented for certification necessarily as a complete package, to me Dixie's point about interfacing or interacting with the privacy and security, you know, the modules being able to plug into or draw from the appropriate security technical functionalities that are present in other modules that altogether constitutes the base, it seems to me like it's still an open question without sort of understanding what is a base and how does it get certified as a base, etcetera?

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Deven, this is Joy. We will get you information on that and send it to you. I will be honest and tell you that is so far down in the weeds that from my experience with this rule that I really can't answer it.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

And the people who can answer it are not on this phone call. I mean, I could ask Steve Posnack that question and he could give me the answer in 10 seconds.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Is Mike Lapinski on the phone call by any chance? Hearing nothing I take it as a “no.” So, we will get you that answer. So, the question is you want some more information about how a base EHR is certified and whether it is presented as a package?

Paul Egerman – Businessman/Entrepreneur

Yes and also how it is defined. What is a base EHR? How is that different from a complete EHR? How is it certified?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

There is a third concept that we need to throw in this package, I'm just scanning this, is this qualified EHR, you know, you've got a complete EHR, you've got a qualified EHR, you've got a base EHR. I think the qualified is the one that, you know, they present for Meaningful Use, but...

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

No, Dixie, I'm sorry, but the base and the complete EHR are both subsets of a qualified EHR.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah, so I agree with asking for clarification.

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

This is David, I'd like to know what feedback they got that caused them to change this, in other words, my guess is that they heard something fairly convincing to make this fairly fundamental change and what did they hear?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Well, one of the things is our Privacy and Security Workgroup suggested that their idea of certifying every single module against all of the privacy and security certification criteria did not encourage, you know, integrated security functionality across an enterprise. So, that's one and then the other one is these complaints from the vendors. So, that was on Deven's slide actually.

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

Right, so what aspect of that are we disagreeing with, Dixie, because it was our suggestion?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Oh, they didn't follow our suggestion. What we said is when a module, and we spoke only to modules, we didn't talk base, qualified or anything else, but we said when an EHR model is presented for certification it should not be required to be certified, it should either implement all of the security requirements or it should demonstrate that it can integrate with an enterprise security service.

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

So, it's that latter part to demonstrate that it can integrate that you consider is missing?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

This is Joy; I also do know that there was some mention made that testing some of the criteria can be difficult.

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

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah.

Paul Egerman – Businessman/Entrepreneur

So, we're doing the right thing I think if we get some information, because I don't think we're understanding correctly what the rule is and what the problem is that we're trying to solve.

John Houston – University of Pittsburgh Medical Center – NCVHS

I think admittedly though, this is John Houston; there's also confusion by the provider community. They have of these pieces, all these different things that they use to deliver healthcare and there's always confusion as to what needs to be certified, how do I certify certain things, you know, how do I attest to it and so I think there is general confusion at that level too as to how this certification works and what do I need to do.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Businessman/Entrepreneur

Well, that's what drove this I think, because users would purchase a complete EHR, choose not to use one module, purchase a module from somebody else and the complete EHR certified the module that they purchased was certified, but they don't end up with a qualified EHR, because of the way it works, because then they would say, well a complete EHR wasn't certified because there was a module that was missing. In other words once you take the module out it's no longer a complete EHR. So, everybody was very confused.

John Houston – University of Pittsburgh Medical Center – NCVHS

I think that the reality here too is the fact that providers would go to vendors and say "do you have a certified EHR" and the vendor would say, you know, "I don't qualify or I'm just a module, or I'm just one piece and I'm reliant upon, you know, some other system in order to meet that certification" which...

Paul Egerman – Businessman/Entrepreneur

That's true, although I think some vendors would just answer that question and say "yes."

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

John Houston – University of Pittsburgh Medical Center – NCVHS

You're right, but some of them will throw up their hands too.

Paul Egerman – Businessman/Entrepreneur

So, I'm looking at the clock and we have like 6 minutes.

Deven McGraw – Center for Democracy & Technology – Director

Yes, me too. So, we'll get some additional information on this just to give you folks a heads up for what issues are coming down the pike, we'll do the work up off-line on the portal issues, we'll get more information on this one, we have got to deal with a recommendation that we made about the EHR technology being able to at least functionally meet the advanced authentication requirements of the DEA authentication rule, which was expressly not included in the proposed rule and we will talk about that. We'll talk a bit about our recommendation on digital certificates and in particular the testing of those certificates, which we wanted to have done in certification in our recommendations, but that didn't get included either. And then we've got some work to do on patient matching.

So, we have our work cut out for us. We will endeavor to try very hard to try to get questions answered and make some headway on these issues with strawdog recommendations for folks so we can spend less time on the call and more time making progress, but I still think even in an hour we did okay today. And, so with that we should open the call for public comment.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Thanks very much Deven and Paul. Operator, would you open the lines for us please?

Caitlin Collins – Altarum Institute

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

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. Paul do you have anything you want to say to close?

Paul Egerman – Businessman/Entrepreneur

No, I think it was a very good meeting. Our next meeting is on April 9th, is that correct?

Deven McGraw – Center for Democracy & Technology – Director

I think so.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

It is, it's April 9th 1:30 to 3:00 o'clock.

Deven McGraw – Center for Democracy & Technology – Director

All right and since it's not until April 9th we will definitely be trying to make some headway on some of this so that we can use the time on the call to make ideally final decisions. So, thanks everybody and let me know if you like this format of only meeting for an hour. We might have to have more frequent meetings this way, but I certainly like the length of the call. Let me know what you all think and with that we'll close. Thanks everybody and thanks to members of the public.

Paul Egerman – Businessman/Entrepreneur

Thank you very much.

Deven McGraw – Center for Democracy & Technology – Director

Bye.

Public Comment Received During the Meeting

1. Note that the selected standards in MU stage 2 already support Amendments, as does the standards used by NWHIN-Exchange. No problem. This is built into the Document management lifecycle that is at the core of XDS (and all XD*).
2. The problem with EHR modules is that they are not based on a standards based interface and thus there is no expectation of consistency, integrity, or security.
3. The comments that drove modules --- time re-testing security/privacy functionality when the same vendor does multiple certification with the same product with different features.