

Privacy & Security Workgroup
Draft Transcript
May 17, 2012

Roll Call

Operator

All lines have been bridged.

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good morning everyone. This is MacKenzie Robertson in the Office of the National Coordinator. This is a meeting of the HIT Standards Committee, Privacy and Security Workgroup. This is a public call and there will be time for public comment at the end. The call is also being transcribed, so please be sure to identify yourself before speaking. I'll quickly go through roll and then ask any staff members on the line to also identify themselves. Dixie Baker?

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

I'm here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Dixie. Walter Suarez?

Walter Suarez, MD, MPH – Kaiser Permanente

I'm here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Walter. John Blair? Ann Castro? Mike Davis?

Mike Davis – Veterans Administration

I'm here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Mike. Lisa Gallagher?

Lisa Gallagher – Healthcare Information & Management Systems Society

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Lisa. John Halamka? Chad Hirsch? Jeff Jonas? Ed Larsen? David McCallie? Joe Moehrke, John Moehrke, sorry?

John Moehrke – Health Information Technology Standards Panel (HITSP)

John's here.

MacKenzie Robertson – Office of the National Coordinator

John's here, thanks. Wes Rishel?

Wes Rishel – Gartner, Incorporated

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Wes. Kevin Stein? Sharon Terry? And are there any staff members on the line?

Will Phelps – Office of the National Coordinator

Will Phelps.

MacKenzie Robertson – Office of the National Coordinator

Thanks Will. Okay Dixie, I'll turn it back over to you.

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

All right. I want to thank you all for calling in today. The only topic on our agenda is the RFI on Nationwide Health Information Network Governance. As governance would imply, the Policy Committee actually has the lead on this review of this RFI, but we... there were two groups, I think only two groups, in the Standards Committee that were asked to look at particular questions in that RFI. And, one of them was the Privacy and Security Workgroup. As I mentioned in the spread sheet, there was really, or the tables, there was really only one that we were asked to give priority to; priority means address these before you look at anything else. Secondary means look at these next. And then today, Deven asked us to do two more, as our priorities, which are questions 22 and 23. So, we'll do those first and then we'll go to those that we've been named for as a secondary reviewer.

I hope you've all had an opportunity to read the RFI. As far as security goes, the RFI does, as David will tell you and end with, it does reflect a lot of what the Privacy and Security Tiger Team has recommended in the past, so, there are very few surprises here. It's really how they put them together. Would any of you like to make any general comments about the RFI before we dive into the questions?

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

Dixie, David McCallie, I joined late, just wanted to let you know I'm on the call.

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

Great, thank you.

Wes Rishel – Gartner, Incorporated

Dixie, I have been out of the country and, in some ways, I still am, mentally. I've heard about an ANPRM and an RFI, are those different documents?

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

There's only one about governance... Oh, I know where you're coming from. It seems that, and Lisa knows this from HIMSS, it seems that a lot of people were anticipating the governance NPRM, the governance regulation draft reg to come out as an NPRM. But, it actually came out as an RFI and in the RFI, they explain that the results, the responses that they get to the questions that they pose in the RFI will be used to craft the NPRM, which will come out a little later. So, this one is a Request for Information and it has a number of questions in it. I don't remember exactly, in the 30's or 40's, a number of questions in it that they posed for the general community.

Wes Rishel – Gartner, Incorporated

I guess I've never understood the difference between an ANPRM and an RFI anyways, so as long as I know I'm not looking at the wrong document, I'm comfortable.

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

Yeah, you'll see it reads very different, it'll read like, "we're thinking about doing X," instead of "you must... the covered entities must do the following."

Wes Rishel – Gartner, Incorporated

Yeah, but... that's...

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

... Type of regulation it reads like, here's what we're thinking about and we'd like your input on these questions.

Wes Rishel – Gartner, Incorporated

Yeah, but I thought that's the same way advanced NPRM works, ANPRMs work. But, anyway...

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

Yeah, just a little different.

Wes Rishel – Gartner, Incorporated

But anyway, as long as it's only an RFI, then I'm happy.

Walter Suarez, MD, MPH – Kaiser Permanente

Wes, I think, this is Walter Suarez, I think the only difference really is the RFI is one step below, if you will, or above an Advanced Notice of Proposal, depending on how you see it, or both, in that the RFI is less, as Dixie pointed out, less prescriptive and a lot more open and leaves a lot more opportunities for the regulator to modify, change, take things out or in, add new things. I think that's the main difference is that this one step below the degree of requirements and takes us from the Notice of Proposed Rulemaking.

Wes Rishel – Gartner, Incorporated

That's good. My main concern was just that I wasn't looking at one document and everybody else is looking at something else, I think I'm okay.

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

Okay, are there any other general comments before we start in the discussion? Have you guys had the opportunity to review it? I know Walter has.

M

I have to confess, I have not, though Walter has told me much about it.

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

Oh, okay. The two fundamental concepts are the conditions for trusted exchange, which they call CTEs, and these are basically requirements, what we'll ultimately see in the regulation is requirements, but they're not requirements that everybody must meet, they're really requirements that validation organizations will use to assess whether an organization can be a Nationwide Health Information Network validated entity, NVE. So, the CTE and the NVE will come up in a lot of these questions and that's basically what those are. There are a number, I think there were 3 or 4, of these CTEs, these conditions for trusted exchange, that were security related; so, I guess as you might suspect. So, with that, we've been given not a whole lot of questions, but let's start with kind of to go in the order that they appear in the document.

Will, you've highlighted... let's start with...

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

Are you ready for me to bring up the document Dixie?

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

Yeah, that would be good. Why don't we start with questions 22 and 23.

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

Okay.

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

And those... I had an opportunity to see these questions a bit ahead of time and I made a couple of recommendations for ones that really hadn't been assigned to us, but I thought we would be good to address them; and, as you heard earlier, just this morning, Deven got back to me on that and agreed that we should be the primary for this question 22 and 23, as well as 57. So. Okay, question 22 is, "Are there HIPAA security rule implementation specifications that should not be required of entities that facilitate

electronic exchange? If so, which ones and why?" The RFI says that the NVE must comply with certain implementation specifications that are designated as addressable in the HIPAA security rule, and so this addresses, I'm not... I don't think it's all of them... Right? Walter, is that right? It's not all.

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

It is all.

Walter Suarez, MD, MPH – Kaiser Permanente

Well yeah, what is happening is there are certain specifications that are addressable and what this is proposing is that the NVE will be expected to comply with these as required, so, turning the addressables into required under this proposal.

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

Does it turn all of them into required, or...

Walter Suarez, MD, MPH – Kaiser Permanente

No, no, only certain ones.

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

Certain ones that, yeah, that are addressable that it turns into required.

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

But for those of us who don't have these section numbers memorized, is there a list of which ones that would be?

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

It's in the RFI, refers to, I'll bring up the HIPAA security rules and Will, if you could find that section... well, you don't have the RFI there, do you? Do you have the RFI available to display?

Will Phelps – Office of the National Coordinator

I do not.

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

Okay, I'll tell you which ones they are.

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

I've got the numbers here, but I don't know what the numbers correspond to.

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

Okay, let me just bring up the HIPAA security rule... the HIPAA administrative simplification, the whole thing. Okay, if you give me the numbers, I'll look them up.

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

So, it's 164.308.

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

That's administrative safeguards, all of those practices like availability, all of the administrative practices, the risk assessment, the risk management, the disaster recover... emergency operations, etcetera. Okay?

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

310.

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

310 is physical safeguards.

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

And, 312.

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

That's technical safeguards.

Walter Suarez, MD, MPH – Kaiser Permanente

You know, come to think about it, I guess what this is doing, reading it again is, it's really incorporating all the requirements from the HIPAA security regulation that are addressable, all of them really. I thought it was only selected ones, but looking at it again, it's really all of them.

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

Yeah, it's...

Walter Suarez, MD, MPH – Kaiser Permanente

...that are addressable becomes required. So, yeah, so out of the 42 implementation specifications in the HIPAA security rule, there are about 15 or 16 that are addressable among the physical, technical and administrative safeguards, and then this is turning all of them, all of them into required for NVEs. So, yeah, I think I was thinking that there were some selective ones, but no, it is all of them.

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

Yeah, I was thinking it was... because I remember their siting numbers, but I didn't realize that's the whole section, but clearly it is the whole thing. And they also require that these NVEs be business associates

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah.

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

So, the question is...

John Blair – Taconic IPA

Hey Dixie, this is John Blair. I thought they talked about them becoming certified entities.

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

Not certified... you mean covered entities?

John Blair – Taconic IPA

I mean, yeah, I'm sorry, covered entities.

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

No, they talk about them being business associates.

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

To behave as if they were covered entities.

Wes Rishel – Gartner, Incorporated

The business associates carry all of the penalties of being a covered entity, as of HITECH anyways.

Walter Suarez, MD, MPH – Kaiser Permanente

The business associate's already subjected to that Wes pointed out. But, a regulation technically is not able to convert an entity into a covered entity, because the covered entity concept comes from the HIPAA law. If the HIPAA law originally, back in 1996, said the only 3 entities that are covered entities are these ones.

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

Well yeah, but a regulation could change that, but they haven't. They have...

Walter Suarez, MD, MPH – Kaiser Permanente

No, I don't think so.

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

They have...

Walter Suarez, MD, MPH – Kaiser Permanente

That's in the regulation, what's in the regulation...

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

They have changed the business associate, they have...

Wes Rishel – Gartner, Incorporated

No, they didn't call them covered entities, they just changed the... they just treat them as if they were covered entities.

Walter Suarez, MD, MPH – Kaiser Permanente

The business associate is in the HITECH Act itself, so it's another law that added requirements for business associates to become pretty much covered entities, but they didn't really call them the covered entities, but it's a law that changed that...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Because there still is some privacy requirements that are not required of them; like the right not to amend, that stays with the covered entity.

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

They have... they are making them business associates.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, that makes sense. Right, and that's what everybody was kind of assuming anyways.

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

Right.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah.

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

So, and it's because of these addressables, which would now be required, in a sense they're raising the bar above what covered entities have to do.

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

That's right.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Not... well, yeah, except that the addressables, the feature of addressable is intended to allow for low scale, and it's very difficult to understand one of these business associates that is a low scale, you know, an entity that has no technology.

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

Mom and pop HISP.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, mom and pop HIE. I don't see it, on its face as being really surprising. The question is, is there something hiding in the detail that's not obvious on first blush.

Lisa Gallagher – Healthcare Information & Management Systems Society

Dixie, this is Lisa Gallagher. My question here would be, if we do that, these are implementation specifications and being addressable there's a lot of flexibility. Do they intend to include some specific standards that they need to meet, since they are now required. I mean, what is that paradigm once we move them from addressable to...

Wes Rishel – Gartner, Incorporated

I have the same question. What is the impact of removing addressability from some of these (indiscernible)?

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

Well, remember that the only things that are addressable are implementation specifications and each one of those is under a standard. So, the standard is already there, it's just that the implementation specification makes it more specific.

Wes Rishel – Gartner, Incorporated

So given what we've gone through, could someone who's familiar with HIPAA, talk about one of the standards and what implementation guides went from addressable to not addressable, at least for these certified entities.

Lisa Gallagher – Healthcare Information & Management Systems Society

Well, I think about encryption. I mean, I think that's a good one to work through, because there was a lot of flexibility there and what is it they want to certify these . . . what is it they want these people to meet as a minimum standard.

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

This is David. Just to throw into the mix, some of these things when you're thinking of an NVE as a large scale existing HIT player, may not be that challenging, but consider that the view, download and transmit implies, I think, that new kinds of entities like personal health records, would be a part of... would become NVEs, so, are there implications on new entities that are too burdensome here, for example, personal health records, mobile health apps.

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

Well, but these NVEs are really exchange agents, they aren't... like covered entities are not NVEs; they are... these are more HISP, various flavors of HISP.

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

But, if you want to be... if you want to host a direct address on behalf of a consumer and receive a secure message from a provider as part of the view, download and transmit activity, aren't you an NVE?

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

You aren't, no...

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

You're a HISP...

M

A HISP is an NVE, right?

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

Yeah.

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

Pardon?

M

I was pretty sure I saw language that said that a HISP is an NVE.

Lisa Gallagher – Healthcare Information & Management Systems Society

Right, right.

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

Yeah, but the NVE is the entity that facilitates that exchange, not the end-point necessarily.

Wes Rishel – Gartner, Incorporated

So the HISP is an NVE, the doctor's office is not . . .

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

Right. But a personal health record would be.

Wes Rishel – Gartner, Incorporated

Yeah, and I, just intuitively, I don't see any reason why a personal health record shouldn't have the same security standards as an HIE, but, we ought to look at it and see if there are . . .

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

Yeah, that's the question I'm raising is just consider that there are new players in this space, that . . .

Lisa Gallagher – Healthcare Information & Management Systems Society

Yeah Dixie, I think we should put the questions here that we have and not make any assumptions about what they're thinking, because . . .

Walter Suarez, MD, MPH – Kaiser Permanente

I think it's a very good, this is Walter, it's a very good argument, I think. We should make a comment about that, the fact that in some cases the addressable standard that's in the original HIPAA regulation does not seem to have a specific . . . I'm reading, for example, encryption; implement a mechanism to encrypt and decrypt electronic protected health information and that's pretty much all it says. Now, the intent, as I recall with HIPAA security, was an addressable standard is a standard that the entity either meets or has to make the argument that it's not reasonable and appropriate to meet and so they have to provide an alternative one to address it. But, here, they are converting them into required and so, I think it's a valid comment to make that in general, this is applicable to all the CTEs in these guidance that are addressable, it will be important to clarify how an addressable requirement becomes an addressable, you know, implementation certification that becomes now required, where there is no specific standard to be met, whether there will be an intent to create more specific guidance.

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

Yeah. What we're saying is that we recognize that some of these implementation specifications will need to be paired with standards to be used just for implementation.

Lisa Gallagher – Healthcare Information & Management Systems Society

Exactly Dixie.

Wes Rishel – Gartner, Incorporated

Okay, so just looking at a summary of HIPAA, everybody who is one of these NVEs will have to have workforce security, including workforce clearance procedure, termination procedures; whereas when it was addressable, they could argue that it was obvious in the office, they have to have information access authorization...

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

Workforce security Wes, is a standard. I'm looking at the HIPAA. That's a standard, so that's not the part that was addressable.

Wes Rishel – Gartner, Incorporated

However, under the standard, there are listed addressable sections, authorization and/or supervision, reports clearance procedure and termination procedures. So, whereas Dr. Bill and Bob might have been able to say, we would know if a fired employee were in the office; Bill and Bob's HISP would have a requirement to get the keys and change the passwords and so forth, when someone left the firm. For the information access management standard, the addressable ones were access authorization, access establishment and modification. For security awareness and training, security reminders and protection from malicious software, login monitoring and password management all become required, where they weren't before. For contingency plan, testing and revising the procedure becomes required and application and data criticality analysis becomes required. For physical safeguards, contingency operations, security plan, access control and validation procedures, maintenance records are now all required.

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

Facility security plans.

Wes Rishel – Gartner, Incorporated

Facility security plan, yes. For device and media controls, accountability and data backup and storage are moved into the required phase. And, for technical standards, automatic log off and encryption and decryption become required. Mechanism to authenticate electronic PHI under integrity becomes required. Integrity controls and encryption on transmissions become required. And, there are no changes to organizational safeguards because the standards are all required, were all required in HIPAA. So, just, obviously there could be some fine print in any one of those implementation rules, but, overall, this passes the sniff test for me. If somebody's going to be an HIE or an HISP, I think they ought to be doing that stuff.

Walter Suarez, MD, MPH – Kaiser Permanente

I mean, that is the question #22. Question #22 says, are there HIPAA security rule implementation specifications that should not be required of NVEs. If so, which ones and why.

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

That's what he's answering Walter. Yeah.

Wes Rishel – Gartner, Incorporated

Yeah, what I'm saying is, at a high level...

Walter Suarez, MD, MPH – Kaiser Permanente

At a high level, yeah...

Wes Rishel – Gartner, Incorporated

There are, none of those titles seem inappropriate for any organization that claims to be an HISP, an HIE or a PHR.

John Moehrke – Health Information Technology Standards Panel (HITSP)

I would certainly agree, on the face of it, it seems very clear that it's not a problem. The question becomes, since we haven't really applied that kind of a rule to anything similar, we're not sure what's hiding under the details.

Wes Rishel – Gartner, Incorporated

Right, I think we need to look...

John Moehrke – Health Information Technology Standards Panel (HITSP)

I think the other...

Wes Rishel – Gartner, Incorporated

Well, the rules have been applied to covered entities that are large, but, I agree with Walter, we need to look at the text of each of those controls and compare them to our mental model of an HIE, and HISP or a personal health record and see if anything looks out of place.

John Moehrke – Health Information Technology Standards Panel (HITSP)

And my understanding of most of the operational HIEs, whether their being direct-based or exchange-based, they are going in as a business associate. So, the other side of this, that I kind of wonder about, is given that our assessment is, you know what, these probably would all be handled appropriately without the change from addressable to required. What is it that they're getting by making that change?

Wes Rishel – Gartner, Incorporated

Well, I'm not clear about the supposition you made as the first part of your question.

M

Yeah, I agree.

Wes Rishel – Gartner, Incorporated

It's not clear to me that business associates can't have, can't use addressability in deciding on controls. And if, for example, we think of an HISP as being a free-standing entity, it may not have all that many employees. So, it may, without this additional regulation, it may have a cogent argument for saying that in the integrity controls is optional; that's probably a poor choice because our standards call for those, but the facility security plan is addressable and this is saying, even though it's Bill and Bob and Bob's mom that are doing this, they still have to have a facility security plan which is fine with me, I think that if their primary job is being entrusted with data, they should have a facility security plan.

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

Wes, one point I want to make is that, you mentioned, well, we already have a standard that requires integrity. It's important to recognize that the EHR standards and certification criteria are for certifying EHR technology. This RFI is more equivalent to HIPAA, in that it does prescribe how an organization is operated, not what it's capable of doing.

Lisa Gallagher – Healthcare Information & Management Systems Society

That's correct Dixie. That's the distinction.

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

It's important to keep that distinction.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Right, so the integrity control is across the whole operational spectrum, not just while it is in any particular...

Wes Rishel – Gartner, Incorporated

Yeah, I stand corrected. That's a good point.

John Moehrke – Health Information Technology Standards Panel (HITSP)

But, I think your overall point is the same as I was trying to make in that the way this stands today, as addressable, I think will drive you to the correct result anyways, and changing them to required...

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

This is David, I'm kind of with John. I would question what do they think... why do they think they need to make this change, what's broken about the scalable addressable approach.

Lisa Gallagher – Healthcare Information & Management Systems Society

And what else might they be thinking of requiring, some specific standard or threshold that they now have to meet?

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

Yeah.

Wes Rishel – Gartner, Incorporated

Well, I mean I need somebody, maybe I still need to be educated here, but, my understanding of addressable is, just to pick one, that facility access controls has some language that says this is what the controls have to be or a citation to another document or something like that, but, organizations that are small, don't have to follow that.

Lisa Gallagher – Healthcare Information & Management Systems Society

Not all of them do, Wes.

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

No, they really don't. The addressable in facility, I mean, the facility standard, access control standard, is implement policies and procedures to limit physical access to its electronic health information and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed. It doesn't specify how you do that. The only cases where it does are these implementation specifications, but even there, the addressable under facilities is contingency operations and facility security plan. I think...

Wes Rishel – Gartner, Incorporated

Well, let's go back then to say, what... is the group saying that...

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

Let me finish my thought because I really am responding to you. I think what you get, and I think it's a valid argument, what you get is predictability. They do a lot in here to make these NVEs predictable, so that... and a covered entity that's considering using one of the NVEs, doesn't have to guess whether they have a facility security plan or not. They know. So, they're trying to eliminate all of the gray or, as many gray areas as they can. And I personally think making these addressable required is one way that they can do that, making it predictable.

Wes Rishel – Gartner, Incorporated

So, can I just restate what you said? There are certain standards that have certain implementation specifications that are currently labeled as addressable. Those implementation specifications, even when taken as required, are pretty non-specific.

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

Yeah.

Wes Rishel – Gartner, Incorporated

So, adding the addressable to those really adds very little in terms of the requirement, except maybe they don't have to have a plan and a book on the wall.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, there's a little more to this. So let me, if I can explain briefly the concept of addressability in more detail, so, and I'm reading from the Rule, so. An addressable implementation specification, a covered entity must first assess whether each implementation specification is reasonable and appropriate when analyzed with reference to the likely contribution to protecting the entities health information and, as applicable to the entity: A) Implementing implementation specification as is or B) If implementing the implementation specification is not reasonable and appropriate, then #1 document why, and #2

implement and equivalent alternative measure if reasonable and appropriate. So, what it means in the physical plant situation is, the entity could say, well, it is not reasonable for us to implement a physical security plant plan and they argue that their physical plant is only one room and that there is no information in it or no computers in it and so, they say the alternative measure is, we don't implement anything; and that is what they can do today. In fact, that's what many people do.

John Moehrke – Health Information Technology Standards Panel (HITSP)

And their only danger would be that they were in an audit, the auditor decided they were unreasonable.

Walter Suarez, MD, MPH – Kaiser Permanente

Exactly.

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

Yeah.

Wes Rishel – Gartner, Incorporated

So, what we've done is said, what this RFI is stating is that for the listed standards and their implementation specifications, we are removing that variability. Frequently, however, the implementation specifications are also written in terms of appropriate levels and that flexibility would still remain.

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

So, do we think it should? Well, we're saying they should add some specification . . . I think that's our answer to this one actually; that would reduce some optionality, but the variability would still be there and so therefore, we think that each implementation spec needs to be paired with some standards.

John Moehrke – Health Information Technology Standards Panel (HITSP)

So, I think I've heard three possible answers from different people in the group.

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

Well, that's what I thought you just said.

Wes Rishel – Gartner, Incorporated

No, no, no. I was observing that, I wasn't saying we needed to change it. So, there are at least two possible answers. I heard David and another person say, effectively, if I understood them, the difference between addressable and required is so nominal, given that the implementation specifications themselves are flexible, that it's not worth changing them from addressable to required. And I took the position, agreeing on the data essentially, that it was worth changing them from addressable to required, because it did reduce one level of variability, one level of an auditor having to override an opinion and in cases . . . and I thought we did need to look at the individual implementation specifications, just to be sure that some one of them might really ought to stay addressable; but broadly, my view is that a PHR or an HISP or an HIE, should be operating at the level of security of a large covered entity, even if it's a smaller organization.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Okay. Yeah, I was the one proposing that the ability to downscale may still be needed and until I see evidence that there is a problem with having the ability to downscale, it's difficult for me to say, we should force everybody to do something that they haven't anticipated doing today, and have unanticipated result. I honestly don't think either answer is better than the other; but, I just . . . I'm not . . .

Wes Rishel – Gartner, Incorporated

And this is John?

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, this is John, I'm sorry, this is John Moehrke. I just don't know if there's evidence to prove that these need to change.

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

And this is David McCallie, I'm with John on that. I think that we don't know enough about what kinds of NVEs will emerge in the future, of a fully connected system with mobile devices and...

Wes Rishel – Gartner, Incorporated

What's the fastest way for us to get a list of the implementation specifications that we could review and ask, does... do we want to require this implementation, or do they really think there needs to be room for each entity to make its own decision on how much of facility security planning it has to do, for example.

Walter Suarez, MD, MPH – Kaiser Permanente

I think, this is Walter, I think that, and I think Dixie has said it a couple of times, I have them in front of me in a table, I can share this table with the group at the end of the call, too. But, clearly, all of them, the common element is that the requirement is to implement policies and procedures to do this; it doesn't say how to do it, but just to do that. So, the facility security plan is a good example; you want to implement policies and procedures to safeguard the facility. Another one is, maintenance of records; implement policies and procedures to document repairs and modifications to the physical components of the facility. Very quickly, another one, accountability; maintain a record of the movements of hardware and electronic media.

All of them, in my view, are clearly expectations that because the NVEs are now entities that are going to be transporting and allowing exchange and maintaining some of this data in probably large quantities, it would be, to use the term, it would be reasonable to expect that they are going to need to comply with all of these addressable requirements by virtue of creating policies and procedures to ensure that all of these addressable requirements are now met. So, my position is, I think it's reasonable to turn these addressable requirements into required requirements. But, the other point is, I am concerned that if we start establishing or ask CMS to establish or ONC to establish the standards for meeting those requirements, we're going to create a set of standards that apply to NVEs for, say encryption that might be different from the standards that are required by others. And so, I would be... I mean, unless we're saying that we have to define the standard for access authorization and it has to be exactly the same for everyone, whether it's an EHR user, certified EHR user or whether it's an NVE, which would be fine too; then we would be doing that, but, I think we need to #1, provide the, in my mind, the requirement to have this addressable implementation specification be required and #2,, allow that definition of what is the actual standard to be still flexible.

Wes Rishel – Gartner, Incorporated

Well, so, every...

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

...sounds like addressable.

Lisa Gallagher – Healthcare Information & Management Systems Society

Well, yeah...

Wes Rishel – Gartner, Incorporated

So, just to restate what Walter said, right now there is some reduction in variability by converting addressable to required; but not much, because the implementation specifications typically just say you much address it, I mean, they aren't that specific. If in fact, NVEs didn't have the option of addressability and regulations were issued that were more specific with regards to implementation specifications, small NVEs would not have the flexibility that small, I'm going to say small healthcare providers, because I don't know that there are that many small payers, but, the small healthcare providers have to be addressable, the small NVEs would be required to meet those future modified implementation specifications. I would say that that would then become a factor on how they wrote future implementation specifications, but, it sounds like it's half of one and six dozen of other right now, in terms of the current implementation specifications; but there is this future contingency that they write more specific ones, where they would have to be careful not to sweep up the NVEs, small NVEs with big organizations.

Lisa Gallagher – Healthcare Information & Management Systems Society

I think that's right...

Walter Suarez, MD, MPH – Kaiser Permanente

Let me just very briefly add one more item. Of all the addressable ones, the administrative and the physical, there's no standard; so, clearly there's no expectations that there will be a need to develop and establish a standard to make it more specific. And the technical safeguards, there's only a couple of them where there are possible standards. For example, automatic logoff; I don't know that there is a specific standard to do automatic logoff, it's a procedural part. Encryption and decryption would be one where it would be helpful to define a standard. And then, mechanisms to authenticate PHI and the integrity, there might be a way to do it, as in the EHR world where we recommend SHA-1 and integrity controls, implement security measures to ensure that electronic transmitted data is not improperly modified, the same as sort of integrity. So, there's only 2 or 3 where there would be some benefit in defining farther the standard, but only of the 16 or 17 addressable, there's only 2 or 3 and all of them are in the technical safeguards.

(Indiscernible)

John Moehrke – Health Information Technology Standards Panel (HITSP)

This is John Moehrke and I kind of want to...

Lisa Gallagher – Healthcare Information & Management Systems Society

May I speak please?

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

Yeah.

Lisa Gallagher – Healthcare Information & Management Systems Society

Dixie?

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

Yes, Lisa.

Lisa Gallagher – Healthcare Information & Management Systems Society

Yes, so I go back to my original comment which is, behind this, the question is do they intend to define any specific standards when they make these required and what would be the process for doing that.

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

Yes, that would be what would make sense. I want to...

John Moehrke – Health Information Technology Standards Panel (HITSP)

So, this is John Moehrke, I wanted to add...

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

I want to clarify that a standard, Walter is using the term standard as a SDO standard; but, there are standards in both the EHR standards NPRM as well in the HIPAA itself that are labeled standards, but are not SDO standards, they're, this is how you do it. So, the word standard is used in these regulations not just exclusively for SDO standards.

Lisa Gallagher – Healthcare Information & Management Systems Society

Correct. I mean...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, this is John...

Lisa Gallagher – Healthcare Information & Management Systems Society

...this is how you must do it kind of standard, or minimum criteria or minimum threshold or whatever.

John Moehrke – Health Information Technology Standards Panel (HITSP)

So, this is John Moehrke. I think there's... we need to separate out a couple of things. Back when HIPAA was originally written, many of the security interoperability standards were unknown, so, they had to leave them very unknown. Whereas today, whether you are speaking of the direct project or the secure SOAP stack or even exchange, there is mandatory security controls built into the protocols themselves. So, from the interoperability perspective, any one implementing one of these standards based communications would be forced to implement those particular transport standards. So that leaves the question of, is there a reason to impose specific operational standards, to use the larger word Dixie's getting to, and that is, standards of practice. And there, I think we do get into the question of, well, once you start defining standards of practice, you will eliminate a lot of useful flexibility; you may actually create some problems. So, I think now that the industry and health information exchange has matured, we have to look at it in that light as well.

Mike Davis – Veterans Administration

So this is Mike Davis. I have a comment as well on this subject, just throw in here, just my take here – it's that it may be that what is desired out of this is not to force the small guys to implement things that are unreasonable and unnecessary, but to provide a greater degree of assurance to their business partners of how they are addressing these addressable items. So, I think I'm looking at it more as in terms of providing trust, level of trust to partners of how they are dealing with things. So, it may be... if it was published sort of like someone would publish their certificate policy, and saying well this is, we don't think that this particular addressable thing applies to us and here's why; it provides assurance that might not otherwise be known to a trusting partner of how they're dealing with that addressable thing. We assume that the ones that are required they're doing, so, that's sort of set. But we don't know about the ones that are addressable. So, by moving them into, you must address them, and provide publically how you are doing that, it provides this kind of assurance that I think maybe they might be looking for.

John Moehrke – Health Information Technology Standards Panel (HITSP)

(Indiscernible) ...the other governance.

Walter Suarez, MD, MPH – Kaiser Permanente

The other point is maybe...

John Moehrke – Health Information Technology Standards Panel (HITSP)

There's a lot of governance in the RFI, that brings up that there is far more than just the HIPAA covered items, so, we really do need to kind of look at it holistic.

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

Yeah.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, the other point that I was going to make is, many of the required ones today are just as equal in terms of the description as the addressable ones, and we don't have standards, as I note, for those. And so, making the addressable ones required and then on top of it, adding some additional definition of exactly how those are to be done, turns the question into well, maybe we then also would need to do the same for the required ones that are today required. So, I would still state, and I think John your argument and my two arguments supports the fact that this indeed should be turned into required as an increased level of trust and minimum expectations that at least they establish policies and procedures for all of these things, but getting to the next level of defining actually how they do it, whether we call it standard or whatever we call it, may be not necessary or not appropriate to do here, because it would elevate these addressable ones into a new level of additional definition of how they are done, and we might need to actually do then the same with all the other ones that are today required.

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

Well, let me remind you all of two things. Number one, they are not asking us whether this is a good idea or not; they are asking us whether there are some of them that should not be required, are there exceptions. So, I will send to you the extract from HIPAA and highlight the addressable ones, just so you can just go down there and make sure that there are none that you think are big showstoppers. The second point is, with respect to these details, if you think about the context for what we're discussing here; we are talking about what an organization must do and the basic requirements they must meet when they come to a validation organization to get validated as an NVE. Just like with EHR certification, that validation authority, that validation organization will have procedures that they put in place that will have to be more specific than what's in the law now. So, that will have to be developed as part of validation and the validation procedures and specific criteria that they use will have to be consistent, but they wouldn't have to be in the law itself.

Walter Suarez, MD, MPH – Kaiser Permanente

You're talking about validation procedures for the network validated entity, the NVE?

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

In NwHIN, the NVE has to be validated with a validation organization, just like the certification organization. So, just like the certification organizations have test procedures, these validation organizations will have to have specific criteria and specific ways of determining whether they meet the requirements. So, that rule doesn't have to be in the law itself, it has to be there, but it doesn't have to be in the law itself.

Walter Suarez, MD, MPH – Kaiser Permanente

You mean in the regulation, not the law.

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

Well, a regulation is a law, yes.

Walter Suarez, MD, MPH – Kaiser Permanente

When we're talking about regulation here...

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

I know, in the regulation, you're right.

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

But these are operational requirements, not certification requirements.

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

They are validation requirements, yeah...

Walter Suarez, MD, MPH – Kaiser Permanente

So, a validator would be...

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

The way the RFI model is defined, is that an organization would go to a validation authority, I don't remember the... validation organization. What ONC is proposing is that they create a set of validation organizations, a whole structure of validation that is very, very similar, and they call it that, that is patterned after what they do with EHR technology; but in this case, they would validate organizations to be NVEs.

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

Yeah, but a validation is a static snap shot, these are operational requirements.

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

I know, but that's what they're validating are their operational requirements. It's just like if you did a validation for HIPAA, only in this case you're doing a validation that they can be NVEs.

Walter Suarez, MD, MPH – Kaiser Permanente

It says in the rule that the HIT Policy Committee defined the term or noted the term validation to refer to the process of verifying compliance and it may include a broad array of possible methods including self-attestation, testing, certification of systems; so, that is to be defined...

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

No, no. Walter, that is defined in the RFI. They say they're going to set up a system that's just like what they do . . . the ONC will set up a system just like what they do with EHR technology. They don't leave that hanging out, no.

Walter Suarez, MD, MPH – Kaiser Permanente

No, what I meant, that is to be defined, is the actual methods by which they will be validating NVEs...

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

Yes, yes.

Walter Suarez, MD, MPH – Kaiser Permanente

...that is to be defined, and my point was going to be that, with respect to making some of these addressable required, that one validation could be that the entity checkmarks do have implemented policies and procedures to address physical plant security. They don't evaluate the actual policy and procedure and determine that the policy and procedure is appropriate to the entity, they just validate that they do have policies and procedures. So, that's a question as to which level... to which degree the validator, the accrediting body of NVEs will go inside and disaggregate the actual policies and procedures and say, this policy doesn't seem to be appropriate for a new entity that has a mainframe system or something like that. So, I just wanted to make that...

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

Well right, and that will have to be worked out. But, I don't think that that should be in the regulation itself, that...

Walter Suarez, MD, MPH – Kaiser Permanente

I agree, I don't, exactly...

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

...they need to build.

Mike Davis – Veterans Administration

But if you're looking for this good housekeeping seal of approval when the certification body comes in and they ask them a particular thing, and the certifier... the claimant says, well this doesn't apply to us, and here's why; the certification entity doesn't have to say, well, you have to do it anyway, whether it applies or not. That just doesn't make sense, it should be...

Walter Suarez, MD, MPH – Kaiser Permanente

It will be if they return this required, as they are proposing, the entity will be required to address them, I mean address them is not the right way to say it, they will be required to do them.

Mike Davis – Veterans Administration

The question that we have, isn't it, I heard Dixie say, was among those things that are addressable, are there some that we don't think need to be addressed, so that the certification entity wouldn't even have that on their list.

Walter Suarez, MD, MPH – Kaiser Permanente

But you're argument is that all of them should be...

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

To be specific, what they're proposing is that ONC will create a single body to accredit and oversee validation bodies and these validation bodies, that's the term that they use, are those that will validate the NVEs that they... that their operations conform to this regulation.

Walter Suarez, MD, MPH – Kaiser Permanente

So, Mike, your argument is, it sounds like, that we should not be selectively saying this one makes sense to be required and this one makes sense to still keep it addressable; that really all of them should be required to ensure the level of trust. Is that accurate?

Mike Davis – Veterans Administration

No. I think, I mean, in terms of the certification thing, I think, my interpretation of the question would be that we would look at the addressables and say, well, these don't need to be... this addressable one does not need to be considered by the certification body.

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

That's exactly what they're asking Mike. And I think that that's the next step. I'll send you guys the section of HIPAA that... and I'll highlight the addressable, and just do a quick eyeballing and see if you see any that really should be not addressable. And Will, that last sentence you've written is not true, they clearly define how they're going to do validation bodies. Yes, there will be multiple validation bodies and one accreditor of validation bodies. So, you can delete that sentence.

Wes Rishel – Gartner, Incorporated

Well, but that accreditor is also an accreditor of NVEs, right?

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

No, no. It accredits these validation bodies.

Wes Rishel – Gartner, Incorporated

Well, the language talks about an accreditation...

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

Of these bodies, right.

Will Phelps – Office of the National Coordinator

Hey Dixie, this is Will, I will remove that question. I only wrote that last statement because it wasn't asked in the construct of the question.

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

Right. Well, the answer is yes, they do have validation bodies. Here's the way it's termed, "Similar to the roles and responsibilities we established under the permanent certification program for HIT, we could see establishing a process by which the National Coordinator would approve a single body to accredit and oversee validation bodies. The process considered in this RFI, however, would differ from the HIT certification program in that validation would evaluation an entities conformance to adopted CTEs as opposed to a particular product certification and certification criteria."

Wes Rishel – Gartner, Incorporated

Okay, so, what that doesn't say in comparing with the current certification of EHR is what is the source of the detailed specifications for validation? Under stage 1, NIST and ONC were the source of the detailed specification, so very little was left to the judgment of an accredited, certifying body. But are we to assume that there is a similar role in the government for defining, I mean, for certification it's down to the scripts, you will do this and you will find this answer. That's not within the judgment of a certifying body,

they must use the standard scripts and CCHIT found that often the standard scripts were less selective than their own scripts. We need to be clear with regards to the RFI, what will be the source of the detailed criterion that drive the certifying bodies or the validating bodies and how much discretion the validating bodies have. The reason is that if the validating bodies have discretion, there's immediate drive to the bottom, rush to the bottom, because you'll get more validation business if it's costs less to get validating.

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

That says it. So, I think if we combine your point with what Mike's point and others have said about how making these addressable required does build trust and reduce optionality. But, we also think that the accreditor scheme, the accreditation and validation scheme needs to be very clear on how... on the procedures and criteria that validation bodies use to validate NVEs.

Wes Rishel – Gartner, Incorporated

I don't know what it says now, but I'm still confused on what is the event that would cause a previously validated body to be re-validated? Is it a change in the standards, as is the case for certification of EHRs, or should it be something that's done routinely after so many years anyways.

Walter Suarez, MD, MPH – Kaiser Permanente

I hate to throw a wrinkle to all this, but, the validation process that is being proposed, is being proposed as a voluntary validation, voluntary; it's not a required process. In other words, the NVE is not expected to be required to validate against the validator that has been accredited by this one single entity.

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

But they say you can't call yourself an NVE unless you have.

Walter Suarez, MD, MPH – Kaiser Permanente

Well, I don't know how ...

Mike Davis – Veterans Administration

Okay, right. Let...

Walter Suarez, MD, MPH – Kaiser Permanente

Well, I don't know how because the first question, or question #4, which we are not addressing, but, it says, would a voluntary validation approach, as described above, sufficiently achieve the goal expected? And, the intent is that the validation is a recognition of, it's sort of a seal of approval, as Mike noted, it's sort of a good seal of approval, but you don't have to have it.

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

Yes you do, yes you do. They make that real clear, that's the V in NVE.

Mike Davis – Veterans Administration

No, you have to have it in order to be an NVE, what I don't think they make clear is what an NVE . . . what you can't do if you're not an NVE. That is...

Lisa Gallagher – Healthcare Information & Management Systems Society

Right, that...

Mike Davis – Veterans Administration

Is there any reason an HIE couldn't continue to operate without becoming an NVE?

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

They make it clear that they can, and they're leaving that up to the market. They make that really clear, but they leave it up to the market, you know market competition. If you're an HIE out there and you aren't

labeled, you don't have the NVE seal of approval, they aren't suggesting that you can't operate, they're saying, we're hoping that nobody uses you; that's what they're saying.

M

Right, and that's the question on voluntary.

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

Um hmm. Yup.

M

If we want to have a point in this agenda where we talk about that specific, the wisdom or the effectiveness of a voluntary process, I'd be happy to speak at that, I don't know that we're there right now in our agenda.

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

That's not one of the priority questions, but, why don't we move to the next question.

John Blair – Taconic IPA

This is John Blair, can I just say one thing. I think that under the validating bodies, there contemplating or thinking about a certification process like, as you talked about before, specific on standards, etc., and an accreditation process, separate...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yes.

John Blair – Taconic IPA

...that would begin then into what Wes talked about, moving to the lowest common denominator, so I think they're thinking about both.

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

But yeah, but the accreditation would only accredit the validation bodies. The accreditors would not accredit NVEs.

M

This is where this gets confusing. I think that yes, there is an accreditation, an overarching accreditation and validating bodies, but validating bodies they're thinking of two types.

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

Really?

Wes Rishel – Gartner, Incorporated

Right. Yeah, that's where I was getting confused too. One is more organizational and governance of the body and things like that and the other is more technical and subject to validation by testing and so forth.

M

Exactly.

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

They say that...

M

Hey Dixie...

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

...validation to all the CTEs an entity would be recognized as an NVE. I don't see two here at all. I don't know where...

M

Well, I've been on a couple of the other of these groups and they made that clear and they talk about specific testing and refer to that, and then accreditation, that's . . . again it's confusing, because as you've said Dixie, the overarching accreditation entity would accredit the validation bodies. They do talk about both of those pieces within the validating body part.

John Blair – Taconic IPA

Yeah, it's possible. It's possible that they're actually using the term accrediting at two levels, it's also possible that the people on the other calls, because I was on some of those calls, have picked up the word accrediting because that's what the current whatever that, there's a body that does it now, a non-profit, what is it called, INAC or something like that.

M

It's INAC, yes.

John Blair – Taconic IPA

INAC, right. They use the term accrediting for what they do and that call was dominated by, at least the one that I was on, dominated by someone from INAC, so they may have used the word accrediting just colloquially rather than as a quote out of the actual . . .

Walter Suarez, MD, MPH – Kaiser Permanente

I agree with Dixie. I don't read two types of validation bodies, there's just two steps, one is the accreditation body to be named, so let's say this INAC, I mean whatever . . . whoever it is, that's one body and that body, the only thing it does is certify validation bodies.

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

It accredits, the word that they use, it accredits and oversees validation bodies. And then it says, the validation bodies, upon accreditation by the accreditation body and authorization from the National Coordinator, would subsequently perform the validation of entities conformance to adopted CTEs.

Wes Rishel – Gartner, Incorporated

So this is like ISO standards, you know, ISO-9000 and 23,000 right.

Walter Suarez, MD, MPH – Kaiser Permanente

It goes farther and actually says that that validation, as I think I mentioned before, would encompass many methodologies and that ...process could vary depending on the type of CTE and the potential burden the validation methodology would impose. So, there's a lot of unknown and flexibility on exactly how the validation process itself would work, in terms of the methodology to be used, and that's where the requirement of looking inside would happen. So, I don't think there is any question we're going to be addressing here about the details, but, at some point it would be helpful to provide kind of a comment. There's a lack clarity around that.

Wes Rishel – Gartner, Incorporated

Could you remind us Walter what a CTE is?

Walter Suarez, MD, MPH – Kaiser Permanente

The CTE is the...

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

Conditions of Trusted Exchange.

Walter Suarez, MD, MPH – Kaiser Permanente

There you go, that's... those are the various requirements.

Wes Rishel – Gartner, Incorporated

So, that's pretty close to an implementation specification in HIPAA, isn't it.

M

Yes.

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

Yeah, yeah it is. You know, there are two levels that are... that I think this group would... levels of optionality or kind of grayness; the one that we just mentioned is the voluntariness of the validation of becoming an NVE to begin with. But the second thing is these CTEs are established; they define them as individual requirements basically, but, they don't say every NVE has to meet every one of them; but, an NVE would pick and choose which ones they would conform to. And they also mention that there probably will be a baseline that all of them will meet, but there will also be others that they may or may not, kind of picking and choosing among them as well.

Wes Rishel – Gartner, Incorporated

And is there implication that the CTEs would be defined in the regulation?

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

Yeah, they name them in the... yes.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, a CTE is sort of a, excuse me, a CTE is a base requirement or base expectation, let's call it that way, base requirement. For example, and we'll get into some of those, there are an... an NVE must comply with sections 130-64.308 are the ones that we're dealing with; that's a CTE, that's a statement that an NVE that it... NVE must comply with these sections, is a CTE, is an condition of trusted exchange, they must meet that.

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

Here's one of them, let me read you, an NVE must only facilitate electronic health information exchange for parties it has authenticated and, oh, I picked a bad one but, authenticated and authorized these are directly rendered. It's like a requirement.

Walter Suarez, MD, MPH – Kaiser Permanente

It is.

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

It's a standard in HIPAA kind of.

M

But Wes, to your (indiscernible), it says establish of a process that could be used to adopt, revise and retire CTEs, as they are no longer appropriate. So, they won't have a lifecycle.

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

Yeah, but he's asking about...

Wes Rishel – Gartner, Incorporated

Okay, so they don't come from government regulation, they come from some other body which is the governance body?

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

No, they will be in the regulation.

Walter Suarez, MD, MPH – Kaiser Permanente

They will be named in the regulation, I agree.

Wes Rishel – Gartner, Incorporated

So how can something that's named in a regulation be required by... be retired by a process?

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

The regulation needs to be updated.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, it would be a new regulation that retires when they're not...

Wes Rishel – Gartner, Incorporated

So, when they say establish a process, that process may very well involve issuing new regulations.

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

Wes, this is Mary Jo, folks, this is Mary Jo, and I did just send you all the summary lists of all the CTEs so you can see exactly what they are, and we also want to establish the process in regulation. So the process would be stipulated as to how we're going to assess these for both prospectively for their maturity to add new ones, but also what is the process by which we would either revise or sunset them, or add new ones. And, once they had gone through that process, which was itself stipulated by regulation, then the new conditions would be issued through a new updated regulation. It is anticipated that this will happen periodically, possibly every two years I think is one of the possibilities that's there.

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

Yeah, it's kind of equivalent Wes to if, with the EHR standards, if we wanted to update one of those standards, you'd have to go back to the regulation . . .

Wes Rishel – Gartner, Incorporated

Yeah, I know, I understand that description. The reason I'm . . . there's two reasons why I'm questioning whether there was an alternative in mind. One is, that through all of the work on the NWHIN, there's been talk of a governance board that could set standards that was not... that did not use regulations, so, maybe that's gone now in this RFI, which is okay with me.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, Wes. I also would like to question whether it's appropriate to put governance in the regulation or to have the regulation require compliance to the output of an identified governance body.

Wes Rishel – Gartner, Incorporated

Well, it's just that the... I mean, I suspect that their lawyers told them that creating a governance body was, in effect, creating an entity of dubious legal standing or something like that. But, I don't know that.

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

Wes, I would point out, this is only an RFI, and I believe there are several points in the RFI where there are questions which ask for input on what the process should be. And so, this is only an RFI at this point; so, if your workgroup has strong feelings about the appropriate way to accomplish this, then it is perfectly appropriate for you to make that comment.

Wes Rishel – Gartner, Incorporated

Yeah.

Will Phelps – Office of the National Coordinator

Hey Dixie, this Will. I'm trying to summarize what everyone has been saying.

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

Yeah, I think you have in that last sentence there.

Will Phelps – Office of the National Coordinator

Okay, I'm trying to keep it within the context of the question that was asked, so I just want to make sure that you are happy with the response that is currently there.

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

Well, we'll go through it later, but I think that last sentence, making addressable required builds trust, but, the validation scheme needs to be clear is where we're converging here.

Will Phelps – Office of the National Coordinator

Okay.

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

I will still send to you the section of HIPAA, just so you can just go down and look at those addressable and if any of you have any qualms about any of them, raise them then, but I think this is where we've converged. Why don't we move on to the next one, which is the security, right next to it, 23. Security frameworks. "Are there other security frameworks of guidance that we should consider for this CTE?" Let me look up what this CTE is, we've lost the context.

Walter Suarez, MD, MPH – Kaiser Permanente

This is a CTE that defines that all these addressable are required.

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

Oh yeah, this comes right after it, yeah, yeah. The CTE to read what the specific CTE is that both of these questions address is, "an NVE must comply with these sections of HIPAA and if it were a covered entity and must treat all implementation specifications included within these sections as required." So, both #22 and #23 refer to that. So, are there other security frameworks or guidance that we should consider for this CTE. Should we look to leverage NIST IR-7497, security architecture design process for health information exchanges, if so, please also include information on how this framework would be validated. Is anybody intimately familiar with 7497?

M

No.

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

Does anybody . . . anyone?

Mike Davis – Veterans Administration

Is that the NISTIR?

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

Yeah. NISTIR.

Mike Davis – Veterans Administration

Yeah, I think John and I are familiar with it. This was done by Kevin Stine and the NIST folks during HITSPs activities and what you see in there is a lot of stuff that reflects back on the HITSP work as an overall architecture, which it claims to be, a framework, I think it's quite useful, but, I would argue that there's a lot of water that's gone under the bridge, it needs a refresh. In my opinion, it doesn't adequately address trust management, federation, data segmentation, data masking, privilege management and it's sort of a pre-direct thing, it's really focused on exchange. But, I like it. It's a good baseline for considering how you would do it.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Thanks Mike. I forgot what that was, so yeah, that is . . .

Mike Davis – Veterans Administration

I knew you knew it.

John Moehrke – Health Information Technology Standards Panel (HITSP)

It's framework, yeah, it's a framework that leverages the HITSP work, so, it's going to be out of date from the standards that the current ONC would want to point at, but, I don't think there is something in that vein available, and I think this might also indicate . . . I don't think it's out of date, I don't think it's wrong, but it just, better guidance could be written and I know you would certainly have to augment it with what's coming out of S&I framework under data segmentation. So, I think it's a good foundation.

Walter Suarez, MD, MPH – Kaiser Permanente

So this is more into the future, this could be one of those things that could be added in the review process and update and retirement process. But, it's not mature enough, I agree. I'm not that familiar with this and I can't see how this could be incorporated into additional requirements above and beyond the ones that are already specified in the HIPAA security regulations.

Mike Davis – Veterans Administration

This is Mike. I think it's good guidance. I'm an architect for the VA, I use this document, all right. This is sort of my baseline, the process is there again, it's the architecture that we create to ensure coverage of the things...

Walter Suarez, MD, MPH – Kaiser Permanente

Advising, what you say Mike is great, its guidance.

Mike Davis – Veterans Administration

And NISTIRs are generally not...NISTIRs, unless they're cited in a FIPS are never intended to be more than that, I don't think.

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

And I also think that if they went the route of really telling people how to do architecture and design, I think that's beyond what a regulation should do. I think people would really...you'd get a lot of pushback if you start getting too specific.

Mike Davis – Veterans Administration

NIST has several things in this area that...for design of secure systems that federal agencies have to apply to...have to comply with. So, for Federal Agencies, this is not a big leap, I don't think. And this one is specific to the healthcare vein, like...

John Moehrke – Health Information Technology Standards Panel (HITSP)

It is.

Mike Davis – Veterans Administration

...it was specifically developed like we mentioned, out of the HITSP work, and I think it's still applicable today, though it does need more...

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

...more guidance.

Mike Davis – Veterans Administration

...refreshment.

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

So, to answer their question as are there other frameworks or guidance that we should consider for this CTE, we're saying no.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Are there other guidance at this point in time, no. But S&I framework is working on some.

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

So, why don't we say that some of the work coming out of the S&I framework could provide good guidance.

Mike Davis – Veterans Administration

Good additional guidance, I think. This is Mike.

M

Indiscernible.

Mike Davis – Veterans Administration

There are several areas that it needs refresh in. Yeah, I do too. I mean, it sort of misses the whole end-stick concept, it doesn't address federation. Like I said, its very exchange oriented. I don't think it goes into trust management and privilege management as much as I'd like to see, that kind of thing. That doesn't mean it's bad.

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

Is it more process or is it more architecture design?

John Moehrke – Health Information Technology Standards Panel (HITSP)

It's architecture. It's a health information exchange architecture document. So it explains how you would set up a health information exchange using the HITSP specifications.

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

That sounds very old think to me. I haven't read it, I'd like to review it, but, we don't want to lock in . . .

John Moehrke – Health Information Technology Standards Panel (HITSP)

Well, it's...

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

...what made sense 5 years ago.

Mike Davis – Veterans Administration

It's not prescriptive in that sense, it's a guideline and it contains a lot of useful information and definitions of things that are applicable today. We're always arguing about what things mean, so, in an architectural context, this explains some useful things.

John Moehrke – Health Information Technology Standards Panel (HITSP)

So David, it certainly does not cover a direct project based architecture, so, we'll certainly have to indicate that they would need to point at direct project based architectures, but, it is a high level architecture that does describe the NwHIN exchange.

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

But it doesn't sound to me like something that belongs in a regulation.

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

Right. I agree.

Walter Suarez, MD, MPH – Kaiser Permanente

Well, I think it's worth mentioning that it's good guidance, not to be mentioned in regulation, or to reference in the regulation as guidance only, but not as a requirement.

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

I wouldn't even mention it in the regulation. I think the regulation should really be focused on the requirements. And I wouldn't mention anything else in the regulation either, you know, because the implementation guidance will... needs to be allowed to evolve over time.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, and I think where they're going today with the harmonized specifications, is probably the better place to point at, and this doesn't conflict with those, but it may send a message that sounds conflicting. So, I think I'm with you Dixie, it's not going to hurt directly, it may hurt indirectly. It's not going to help directly, and it may... so, I think it's not a bad thing, but it's probably not going to help enough in order to stamp it into regulation.

Mike Davis – Veterans Administration

Right, I agree with that, too. Am I speaking? Even in the VA we don't take this as a classification to be implemented as a mandatory thing at all. It's purely a...

Walter Suarez, MD, MPH – Kaiser Permanente

I think, I mean, I'll go with that, I think that in regulations, usually guidance don't show up in regulation as much, because guidance is guidance and is more of a reference document. Then later, after the regulation, the regulator could mention...

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

Point to... yeah. Yeah, I agree. Let's go to the question, what 58, the first one... 57, the first one, Will... and this is, no keep going, back to the first... beginning. Yeah, question #57, right there, yeah. "Should one or more of the performance and service specifications implemented by the participants in the Exchange be included in our proposed set of CTEs? If so, please indicate which ones and provide your reasons for including them in one or more CTEs. If not, please indicated which ones and your reasons (including any technical or policy challenges you believe exist) for not including them in one or more CTEs. This is...

Walter Suarez, MD, MPH – Kaiser Permanente

This is under the Request for Additional CTEs section, yeah, section E.

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

Yeah, that's what I was going to just look up. Yeah, this is it. So, this is not under a specific CTE, there's a whole section that talks about Request for Additional CTEs and whether we think we need additional CTEs.

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

Are they talking about something like a service level agreement by this term, performance and service specification?

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

Yeah, I think they're talking about like the DURSA, right? I read DURSA when I read that.

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

Oh, I was reading more like a response time requirement or uptime requirement.

Walter Suarez, MD, MPH – Kaiser Permanente

Exactly, I think that is what it is getting more into, is some expected minimum level of . . .

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

Aren't those in the DURSA though?

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, those are in the DURSA today, so, I think certainly looking to the DURSA as a good starting point and then finding explicit gaps should really be the approach, because the DURSA has been built based on operational standards as well. And it's actually being augmented now, right now as the Exchange is formalizing their certificate policy, so they're updating... that's going to update the DURSA as well, once the certificate policy is identified. So, there also evolving it.

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

And that's an important point, I think, is that it has evolved over time, so it has, to a degree, served the test of real operation, it's not just hot off the press, the DURSA that exists today.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Right, which is why, I was kind of pushing back on governance, I don't believe should necessarily be stamped in the regulation. It needs to be able to change with the dynamics of current technology and attacks and needs.

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

But this RFI acknowledges that, that governance needs to change over time, so, it does say that and I think they're trying to include mechanisms that'll make it easier for the governance to change without changing the regulation all the time.

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

But I would, I mean maybe the DURSA is too encompassing in terms of what it includes to use it as a tag that we can know what it means, but, I would think that things like service level agreements would not be a part of a governance model, that's really more of a business competitive advantage and...

Walter Suarez, MD, MPH – Kaiser Permanente

But should it be, that's the... I mean the question...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Not when your businesses are large.

Walter Suarez, MD, MPH – Kaiser Permanente

The question might not be whether it should be put into regulations or not, but more whether there should be a requirement to have a requirement, not defining what is the requirement, but a requirement to include in NVEs to have a minimum level of service and... for example, going to one of the CTEs, S-7 for the safeguard #7, that says "an NVE must operate its services with high availability." That's just a statement, that's the actual, you know, condition of trusted exchange. And so the question is whether high availability should be more defined in some sort of a service level agreement or should it be just left at that high level of definition.

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

That's not what the question asks. The question asks should one or more of the performance and service specifications implemented by the participants in the Exchange be included. So, they're asking...

Walter Suarez, MD, MPH – Kaiser Permanente

But keep reading, keep reading, keep reading, Dixie because in the question, it says, should it be added to specifically any of the CTEs, one or more CTEs, that's what I'm bringing up, is that one of these

performance and service specifications could be added to this one that I just read, high availability, that's what I'm reading.

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

Right, that's what I'm saying, but they're looking at the more finer level of granularity that really requires looking at the DURSA, right?

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, yeah. So, that my question back to maybe John, is, if you think like the DURSA defines what high availability is, then we refer people... we refer the regulator to DURSA to use in each of the CTEs that are already defined in this RFI, to define the performance and service specification. Is that what you were pointing to John?

John Moehrke – Health Information Technology Standards Panel (HITSP)

Well, what I... yeah, I think that's, from a high level perspective, what it was pointing at. To reiterate, I think the DURSA is a good example of what this new governance should be. I'm not saying that the DURSA itself should be anointed as the governance, just simply because there are... certainly there are exchanges that are using The DURSA today, but there are also others who have taken The DURSA and made their own version of The DURSA. So, I think the governance that would be promulgated from HHS and ONC would need to say, these are the qualities of a governance; in that governance, these are the qualities of service level agreements, the qualities of availability, I don't know what all the qualities of a good governance are and therefore you really have this high level requirements of governance, but you actually have the instance of governance within each of the exchanges and they would be traceable back to having the qualities of the overall governance.

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

But I just went through the DURSA and it itself doesn't specify any performance or service specifications. It just gives the Governance Committee the authority to put them in place. It says...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, I think that you're hedging...

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

...performance...

John Moehrke – Health Information Technology Standards Panel (HITSP)

No, I think. The maturity of the NHIN Exchange today is such that they haven't gotten to all of those, the exacting details. That's why it's not something you can just simply say, The DURSA shall be adopted, because it's not mature, but it is a mature start, that's why it goes into ...indiscernible)

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

It has a section called performance and service specifications. But, in that section it has general compliance, like transaction patterns. Each participant... here is performance and service specifications. Each participant shall comply with all of the performance and service specifications applicable to the transaction pattern that the participant implements and maintains, but, it doesn't specify that those must be in a... are those in a separate document?

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

This is Mary Jo, they could be in their operating policies and procedures.

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

Oh, okay.

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

If you'd like, I can work with Will to make sure you get whatever you need.

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

Yeah, I don't think that we can really respond to this without seeing what they are.

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

Okay.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, I agree.

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

Okay, I'll be sure that we can get those for you.

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

Wasn't, isn't somewhere in the, this is David, somewhere in the preamble that they . . . that the governance model that they're proposing was to address some of the scalability problems of the DURSA, that that was a too cumbersome approach and they want to do... make it...

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

Yeah, they did mention that, yeah.

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

So, I mean, I don't think the DURSA is being held out as our role model, it's tough to learn from it, but they want to go past the limits that requiring, N-squared agreements with a DURSA-like model created.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Right, well, and some of the other things that are built into the DURSA that are down that pathway is this approach you just heard Dixie read, which is, that the performance criteria are based on the transaction pattern where, for example the direct project pattern, which isn't really in the NHIN Exchange yet, but the direct project pattern could be seen as having a different set of qualities, so you wouldn't have to have as high of an uptime with direct, just simply because the email queuing environment can deal with many of the downtimes. So, you absolutely have to have at least scalability relative to the network pattern. I'm not sure what other scalability is a problem in the DURSA.

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

I just noticed that in the RFI they've got a link to these performance and service specifications, so . . .

Walter Suarez, MD, MPH – Kaiser Permanente

Dixie, as you're reading from the webpage from the RFI, is it 28.5.58?

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

No, it says here, in the RFI, it says, "the DURSA includes performance and service specifications which the participating members agree to use in implementing secure electronic exchange. The most recent specifications used by participants in the Exchange can be found on ONC's website and then their footnote 44 has a link to it.

Walter Suarez, MD, MPH – Kaiser Permanente

I mean, if you'll read a little farther, if you read a little farther, it says, these specifications often are arranged on different, including specifications for patient discovery, query for documents, retrieve

documents, and that I think is where question #57 comes . . . choose one or more of the performance and service specifications be included.

John Moehrke – Health Information Technology Standards Panel (HITSP)

All service specifications, yeah. Those don't have performance criterias, but they are service specifications.

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

They are service specifications.

Walter Suarez, MD, MPH – Kaiser Permanente

They are service specifications, yeah.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Any you know, like I said before, within the NHIN Exchange, they are continuing to evolve these policies, for example, certificate policy is being written right now following RFC, I don't know what, which is a certificate policy specification; which is actually this exact same thing that direct trust is doing and, there aligning quite nicely from a certificate policy perspective, based on the differences in type of transaction. So, this is something they also ought to make sure is clear, is that governance does continue to advance and evolve.

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

Yes. It's odd that they ask whether that these... if they're talking about the service specifications, that should they be included in the CTEs, because the CTEs are a very, very different level of abstraction than the exchange specifications. It's kind of an odd...

Walter Suarez, MD, MPH – Kaiser Permanente

But an interesting question, I guess, is that there's no CTE, like even in the business practices section of the CTEs that require that they NVE establish and use a DURSA-like, you know, agreement with the participants. I don't know that I saw that as one of the expected requirements of an NVE.

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

So do you think that's what... I don't think that's what they're asking for here though, right? Because they're asking the specifications, should they be included in the CTEs?

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, that's true... or choose one of the CTEs... well I know this question might be, but that's a different question, whether one of the CTEs should be that the NVE should have a defined...

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

DURSA.

Walter Suarez, MD, MPH – Kaiser Permanente

...DURSA-type thing, because I didn't see that, and that seems to be one of the most critical elements of an NVE to operate, is to have a DURSA-like...

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

But, I thought the model was to move more in the notion that direct trust is moving in, where you establish your qualification to be an NVE, but you don't have to have direct contractual relations with any other NVE to participate in exchange; unlike the DURSA, where everyone has a contractual relationship with every other participant.

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

That's exact – yeah, that's right.

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

We don't want the DURSA model, that doesn't scale.

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

They do say that the NVEs have to publish their policies and practices, privacy policies and practices and use of data and that kind of thing. But, I don't know that it says they have to publish their performance or availability or anything like that, do they? I don't know.

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

Yeah, I don't know either, but I would think that things that are strictly performance service level agreements would probably not be something you'd want to put into regulation or a CTE, other than, I'll hate to say it, in the addressable sense, that it must be high availability.

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

Yeah, and you might have something that says they have to publish their service level agreements or something.

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

Yeah. No, that's a fair point.

Wes Rishel – Gartner, Incorporated

Transparency, I think, both on what's been agreed to and performance against the agreements, can only be good, right?

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

Yeah, I... yeah.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, I agree. Yeah.

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

I think, yeah. That's a good part to... point to include. Transparency of SLAs and their performance against SLAs.

Walter Suarez, MD, MPH – Kaiser Permanente

Is that what we're proposing, a new CTE and maybe business practice, that an NVE must provide their performance level information?

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

Yeah. They publish if their... make their service level agreements you know, public, and their performance against the SLA.

Walter Suarez, MD, MPH – Kaiser Permanente

So that is a new CTE that we're proposing to have.

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

You know, I don't know, because I haven't been through all the CTEs, I haven't been beyond the security ones. It may already be included in the business practice CTEs. Have you been through all those Walter?

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, I've been and you can go to page 28, site 58, and that has a simple, very simple table of all the CTEs.

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

Okay.

Walter Suarez, MD, MPH – Kaiser Permanente

And there's none that describes the kind of...

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

Oh yeah, are you looking at the federal register version?

Walter Suarez, MD, MPH – Kaiser Permanente

Oh, I'm sorry, yeah the federal register version, I'm sorry, yes.

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

Oh, okay, I haven't even looked at that one yet.

Walter Suarez, MD, MPH – Kaiser Permanente

But the other one has a table like that too.

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

Yeah, I see, it does. I see it, yeah. Yeah, I think that that's a reasonable CTE. The value... I mean, if you're going to be very... and it's consistent with their CTEs, they require that you make your practices with sharing data transparent, they should make their services transparent as well. Service...

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah.

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

Let's see, we are... it's 10 minutes 'til. Let me see what all we have. We've done the priority ones. Why don't we look at question #45, just for kicks. That's the next one, it's the very next one. This is about transport methods: "What type of transport method standards should NVEs be able to support? Should they support both types of transport method standards or should they only have to meet one of the two as well as have a way to translate?"

Walter Suarez, MD, MPH – Kaiser Permanente

Dixie, this is just for a reference, this is under a CTE called... the #1 CTE, the first CTE of the second category of CTEs, the conditions for trusted exchange interoperability CTEs. The CTE itself says, "An NVE must be able to facilitate secure electronic health information exchange in two circumstances: One, when the sender and receiver are known and two, when the exchange occurs at the patient's direction." And so this question 45 comes under that category. That CTE.

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

This is David. It makes me nervous to get so specific about these transports that happen to be of focused interest today. It may be that you could endorse these as exemplars that are considered adequate, but you wouldn't want to preclude the emergence of additional standards, as we, technology moves forward. And I also wonder about whether somebody like Surescripts would want to consider itself an NVE, because it is, in fact, performing trusted healthcare exchange, albeit not using either of these two standards, although in a regulatorily approved way. This seems to specific to me.

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

I agree with you, because the direct is a requirement for EHRs to be able to support, but that's not an operational requirement that everybody has to use and these NVEs really are operational. I would think that this would come under the category we just talked about, which is the services that they provide should be transparent and their performance against them . . . to me, I mean you might have an NVE that just is a HISP, you know, that just facilitates direct and you should be able to do that, right?

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

I would say so.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, by leaving it unspecified, it means that they can support one, support two, support many more . . . right?

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

Yeah.

Walter Suarez, MD, MPH – Kaiser Permanente

I agree with that.

M

Yeah, I agree.

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

As long as they make it transparent and they say, here's what I support.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah. That's an important part, is here's what I support.

(Indiscernible)

John Moehrke – Health Information Technology Standards Panel (HITSP)

It would be nice if there was some way that we could mandate that they explain what they support.

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

Well, that's very much related to what Wes suggested in the SLAs, if they make it transparent, the here's what we support, here are the... here's the service levels and here's the protocols that we support.

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

This is David... go ahead John.

John Moehrke – Health Information Technology Standards Panel (HITSP)

What I was going to do was point out that the S&I framework where we worked on the distribution of direct certs and then we continued to define service end-points; that was explicitly for this purpose, so that you could publish what kinds of protocols you support, and direct was one of them, and you could publish in what way you supported, and of course, if you're a direct, you publish the certificates you're an end-point for. So, I think that also supports the use of that set of standards that came out of S&I.

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

But what was that set of standards, what is it called, that we can...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Well ultimately we published that there are two; there is the original for direct project, there is the original certificate distribution through DNS cert records and S&I also identified the use of LDAP...

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

Yeah, LDAP, right...

John Moehrke – Health Information Technology Standards Panel (HITSP)

...with a schema, and that same LDAP with a schema is being seriously looked at by Exchange as a replacement for UDDI, getting way down into the technical weeds, but, they are looking at using that

LDAP spec to replace the UDDI. I can't predict where it's going to go, again, that's way down in the weeds.

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

But the whole idea of using... of establishing a standard for publishing, you know, that should be consistent, it seems to me. The way they publish what they support.

John Moehrke – Health Information Technology Standards Panel (HITSP)

Right, and that was why we did that in the S&I framework, was, we have a generic service end-point definition, for which there is a way to describe the direct end-point and a way to describe other end-points.

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

Yeah.

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

And I think those are both, both of those approaches are good ones and should be supported. I'm reticent to preclude other ones or to force everyone through a certificate-based approach, because I suspect in the future, we'll have non-certificate-based secure approaches that may make sense.

John Moehrke – Health Information Technology Standards Panel (HITSP)

So you know something going on in the cryptography world that I don't?

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

No, but there are a number of people who are not... who are trying to work around the PKI distribution managed problem using web-based approaches, cell phone-based approaches, where you don't possess a certificate yourself...

John Moehrke – Health Information Technology Standards Panel (HITSP)

Well, they're still certificate based. They still ultimately end up at a certificate.

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

Yeah, but where you go to obtain the information might vary, like, we talked about the micro... where they go to find that out might vary. Right?

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

Yeah. I'm just suggesting not being... I mean the goal here is trustworthy...

John Moehrke – Health Information Technology Standards Panel (HITSP)

David, I just want to put you at ease, the LDAP mechanism that came out of S&I framework is not tied to certificates. The DNS cert record is. So, you're arguing for the LDAP mechanism, which was fine with me.

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

Yeah. No I'm comfortable with the LDAP approach; I'm comfortable with the DNS approach for direct, it fits the use case. I just don't want to...

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

...be too prescriptive.

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

I think the focus of the governance should be on trustworthiness rather than on particular technology implementation and standards. I mean, it's a personal bias, but it seems to me that these NVEs, the critical thing about them, is that they are trustworthy; they follow certain rules, they meet expected requirements around protecting the data, integrity, performance, etcetera, but they don't necessarily have

to be predefined by us to be users or any particular standard that we've labeled today as being one of those trustworthy (indiscernible).

Mike Davis – Veterans Administration

This is Mike. I want to push back a little bit on that. Trust is not a binary thing. There's a level of assurance that is associated with trust that has to do with what an entity brings forth, very specifically to a cert, how much they can be trusted in a specific way. So, I think that technology unfortunately, or fortunately, does come into play there. There are certain levels of trustworthiness in today's technology that are only available by certain technologies.

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

But that might change in the fu . . . Mike, I certainly appreciate that, and I think this is a delicate balance and I'm not trying to make too strong of a statement here, other than to avoid premature closure around a particular set of standards that we're all familiar with in early 2012, because things are going to change.

Mike Davis – Veterans Administration

I'm not out here to support a specific standard, I'm just saying that trust is not a binary thing, it's graduations.

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

No, I agree. Absolutely.

John Moehrke – Health Information Technology Standards Panel (HITSP)

And David...

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

Go ahead.

John Moehrke – Health Information Technology Standards Panel (HITSP)

...I don't want to leave you with the impression that I want to stamp LDAP into this particular regulation, I just think that ultimately, at some point, you will have to define interoperability characteristics. I don't think this governance document is the right place to stamp those.

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

I agree. That's my point. That's exactly my point John.

John Moehrke – Health Information Technology Standards Panel (HITSP)

And when I brought that S&I up, I was not trying to imply that it should be put in there, I was just trying to imply that the topic in the governance framework that we're talking about was appropriate and there would be standards to support it, if a lower level specification was meeting them.

Walter Suarez, MD, MPH – Kaiser Permanente

I think we're all in agreement with this question #45, that the regulations should not specify the transport, if I'm understanding correctly, and it is very important to say that, because in the RFI, the RFI says to satisfy this CTE, the CTE about transport, we are considering requiring an NVE to implement and use one of two types of transport specifications; and they mention XDR and XDM and so, I think it's important to make the statement that we believe that the transport methods and standards should not be prescribed in this type of regulation.

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

I think this is a case where the new direction they're going into there's a problem there, I think, because in the case of the exchange model, you've got the coordinating committee that says, okay, here's our transport that we're using, right? In this model, there's no equivalent of a coordinating committee, there is an accreditor that accredits the validation bodies, the validation bodies make sure that their conformant with the CTEs, but there's no entity that says, okay, right now these are the acceptable secure

exchanges. And then, I guess the only way you have to change those over time is to regulation, right? If they want to plug them into the CTEs. Okay, why don't we think about that one, we'll start with that one with our next... at our next discussion. And we're coming up on nine or twelve your time, so why don't we open it up to public comment? And thank you all for dialing in.

Public Comment

MacKenzie Robertson – Office of the National Coordinator

Operator, can you please open the line for public comment.

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 comment at this time.

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

Okay. For our next meeting, Mary Jo, do you know when, or MacKenzie, either one of you, do you know when our next, is it next week?

MacKenzie Robertson – Office of the National Coordinator

It's May 22nd from 10 to 2.

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

May 22nd, 10 to 2. Okay, for that May 22nd 10 to 2, I would like... we've already discussed our priority, and we've started on our secondary, but I would like to have a conversation about something that was brought up in today's discussion and that's about the voluntary approach that they're taking, the voluntary validation approach. We based... voluntarily becoming an NVE versus requiring, because I sense that some of you would like to discuss that and I think it certainly is critical to everything that we do. So, why don't we start off with that more general discussion and then go to our other secondary questions.

MacKenzie Robertson – Office of the National Coordinator

Hey Dixie, this is an update, it is from 12 to 2, not 10 to 2; it's not four hours.

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

I didn't even notice that, I'm "hey, I'm there." Thank you. Yeah, Walter.

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah. No, I think that's a great idea. I think we do need to talk about it and so, I look forward to that discussion.

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

Okay. And I'm going to send you guys the section of HIPAA, so if you just look at all of the addressables, just to make sure that it doesn't change your mind on what we're going to...on our conclusion. Alright. And Walter and I will work with Will to clean up our comments and send them out to you. All right, thank you all very much.

MacKenzie Robertson – Office of the National Coordinator

Thank you.

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

Thank you.

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

Bye, bye.

M

Thank you, bye, bye.