Privacy & Security Tiger Team
Transcript
May 22, 2012

Roll Call

Operator

All lines are bridged.

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good afternoon everyone, this is MacKenzie Robertson, in the Office of the National Coordinator. This is a meeting of the HIT Policy Committee's Privacy and Security Tiger Team. 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 when speaking. I will now take roll and at the end, ask any staff members to identify themselves. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

MacKenzie Robertson – Office of the National Coordinator

Thank you Deven. Paul Egerman?

Paul Egerman – Businessman/Entrepreneur

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Paul. Dixie Baker?

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

I'm here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Dixie. Dan Callahan? Neil Calman? Carol Diamond?

Rebekah Rockwood – Markle Foundation

This is Rebekah Rockwood for Carol.

MacKenzie Robertson – Office of the National Coordinator

Thanks Rebekah. Judy Faulkner?

Judy Faulkner – EPIC Systems Corporation – Founder

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Judy. Leslie Francis? Gayle Harrell? John Houston?

John Houston - University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks John. Alice Leiter? David McCallie?

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

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks David. Wes Rishel? Micky Tripathi?

Micky Tripathi – Massachusetts eHealth Collaborative

Here.

MacKenzie Robertson – Office of the National Coordinator

All right, thanks Micky. Latanya Sweeney? And are there any staff members on the line?

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

Joy Pritts.

MacKenzie Robertson – Office of the National Coordinator

Thanks Joy.

Kathryn Marchesini – Office of the National Coordinator

Kathryn Marchesini.

MacKenzie Robertson – Office of the National Coordinator

Okay, anyone else? Okay, Deven and Paul, I'll turn it back over to you.

Paul Egerman – Businessman/Entrepreneur

Great. Thank you very much MacKenzie. This is Paul Egerman, I want to welcome you to our Tiger Team conference call this afternoon. At the end of this call, there will be an opportunity for public comment. So, I want to say again that the comments from the public are extremely important, so if there are members of the public listening to the call, we appreciate your interest in our work and hope that you will make some comments. What we are talking about this afternoon is some questions that occurred from the Governance Request for Information. A Request for Information was issued and there were a number of questions that were asked and we thought that since the questions were asked, we would do our best to answer them. So, that is what we are going to be trying to do this afternoon. Deven will be taking us through the power point slides and going through the questions.

Deven McGraw – Center for Democracy & Technology – Director

Great, thanks a lot Paul. So, essentially our objective for today is to try to get through as many of these questions as we can. We didn't put them in exactly numeric order, we have definitely priori… put up front those questions that were designated for us as priority for us to answer, but we also have some items that you, the Tiger Team members from our last call, specifically requested be included, which also happened to be assigned to us, but as sort of secondary considerations, but we'll make sure that we get to them. You'll notice on the slide though that we have this call today and then there's a Policy Committee call on the 30th that actually has to do with recommendations from the Certification and Adoption group, related to the second stage of certification; so, that's not something that we're trying to target some responses toward. Instead, what we're aiming for is the meeting on June 6th, because the public comment period for this RFI really ends on June 14th and so, whatever we're able to say, we need to wrap it up and get it into the Policy Committee by the 6th, which means we have today and whatever we can do in between phone calls, and our call on June 4th, to try to get again, as far as we possibly can.

Again, here's just a slide that summaries the focus of our discussion and the relevant questions that we've been asked to address. A couple of things; I hope that all of you were really able to listen to at least one of the presentations on the Request for Information as background. For those of you who haven't though, and for those of you who need a refresher, two key acronyms to keep in mind; CTE means condition for trusted exchange, and that's a governance condition that's been proposed in the RFI

and that is subject for public comment. The other think you need to know is an NVE, which is a nationwide health information network validated entity; these are the entities that have been validated to be in compliance with the conditions for trusted exchange. And so, that's the sort of mechanism of governance that's been proposed in the RFI and it's important to know those two terms.

I think the other thing that it's important to know is that the type of entity that would be submitting itself for validation to be an NVE is one that facilitates exchange, not a provider himself or herself, but an HIE or RHIO or a private network; we called them intermediaries in some of our earlier recommendations. And that's really the type of entity that the governance rule is aimed at. So, with that little bit of background, we're going to go ahead and jump in to the topic of meaningful choice, which is addressed as condition S-3 and then "S" stands for safeguards. There are three categories of conditions and safeguards is one of them; and what's been proposed is that an NVE must ensure that individuals are provided with meaningful choice regarding whether their IIHI, which is individually identifiable health information, may be exchanged by the NVE. And in the other document that we circulated to you in preparation for this meeting, we included language from the RFI preamble, which is the explanatory language, that goes through the rationale from ONC for why they put this condition up there and certainly there are… if you had a chance to read through it, you probably would have recognized a lot of the rationale because it came, much of it was part of our recommendations that were approved by the Policy Committee on the issue of meaningful choice for intermediaries.

And there are four questions that are relevant to this particular safeguard. And the first one is question 27, which is, "In accommodating different meaningful choice approaches, opt-in or opt-out, or some sort of combination, what would be the operational challenges for each approach? What types of criteria could we use for validating meaningful choice, and considering that some States have already established their choice policies, how can we ensure consistency in implementing this particular condition?" Question #28 is, "Under what circumstances and in what manner should individual choice be required for other electronic exchange purposes?" You will recall that our recommendations on choice were limited to the types of information exchange that would be required for Meaningful Use Stage 1, which is largely treatment and care coordination, some public health reporting and… what am I… that's essentially the universe. To the extent that information might be exchanged for other purposes, we didn't necessarily address it in our previous choice recommendations.

Question 29 says that, "Should additional meaningful choice safeguards be considered to address electronic exchange scenarios such as distributed query models that do not take place following the interoperability exchange condition," which essentially… we copied the definition into your document, I think it's intended to refer to directed exchange, but the way that it's defined is when the sender and receiver are known and when the exchange occurs at the patient's direction. But clearly they are referring at least to distributed query types of models, which we didn't necessarily address in our previous recommendations. And then question 30 is, "that the process of giving patients a meaningful choice may be delegated to providers or other users of NVE services as opposed to the patient receiving a choice from the NVE directly, and in those instances, how would the provision of meaningful choice be validated?"

And so what we did here was essentially go back to our initial recommendations that we had made on the topic of meaningful choice, and plugged them in as potential responses to these questions. These answers do not necessarily address every single question that was asked by ONC, but they certainly meet the spirit, I think, of the questions that were asked and cover a lot of the ground that ONC sought to cover and it seemed to make sense to us to sort of start in a place where we had been before, and we can always add to it, if we are able to do that in the time that we have. So, what we laid out here for your consideration is a recommendation that NVE's follow the same criteria for meaningful choice that the Tiger Team had previously recommended, and as noted in the RFI, choice is meaningful when it meets these criteria that are on your slide.

Consistency in approach, whether it's opt-in or it's opt-out is not as important as meeting these specific criteria, which also could be used for validation purposes. And this is again consistent with what we said as a committee back more than a year ago, where we said whether the default is opt-in or opt-out is less important than the choice actually being meaningful, and meeting those meaningful criteria. Then

specifically in response to the question about whether consistency is needed, we have suggested for your consideration this response, that an NVE is required to apply choice with respect to the data sharing that it either performs itself or facilitates between the providers and its network. So consequently, some variation in policy among NVEs is acceptable, and may in fact be necessary in order to accommodate different community norms. I'm just going to go through all of this entire straw man response and then we'll open it up for discussion.

The Tiger Team agrees that choice, beyond of course what might already be required by law, should not be required when an NVE is facilitating secure directed exchange. Remember that we said this in our recommendations approved by the Policy Committee; however, when the decision whether or not to share health information is no longer in control of the provider or the provider's OCA, the patient should have meaningful choice about whether or not his or her information is included in the NVE. Examples of NVEs that should provide meaningful choice include centralized databases, federated models where the NVE controls the data-sharing or NVEs that aggregate data from multiple sources. All of this comes from our previous recommendation letter. When the NVE model is one where choice should be required, patients should have meaningful choice even if the purpose for exchange is for treatment.

And then the last response that we have here, I think it's the last one, the Tiger Team has not yet considered whether… no, it's the second to the last. The Tiger Team has not yet considered whether individual choice should be required for other electronic exchange purposes beyond what the HIPAA Privacy Rule currently requires. The Privacy Rule does impose some authorization requirements for certain uses of data, marketing being one example. And then the last straw response that we have for your consideration is that the Tiger Team has observed that the relationship between the patient and his or her healthcare provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information.

For this reason, we believe that providers should, in most cases, have some responsibility for discussing and documenting patient choice. NVEs should play a role in educating the community about the NVE and its purposes and should give providers resources to help educate their patients and obtain meaningful choice. In circumstances where providers obtain choice, meaningful choice can be validated through an attestation. And again we tried to draw all of these recommendations, either literally or at least in spirit from what we said more than a year ago on this topic of meaningful choice; but of course, we have this opportunity to discuss these responses if they're appropriate, if they're right, if there are things given the passage of time that we would add or subtract, now would be the opportunity to do that. So, thoughts? I just gave you a lot of information. Again, I hope you had a chance to read through this ahead of time, but for those who didn't, I wanted to go through this kind of carefully, so we would all be on the same page in terms of background.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Deven, this is John Houston.

Deven McGraw – Center for Democracy & Technology – Director

Hey John.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I might as well start things off. When I read through it, there was this one phrase that I had concerns about and it was on the last paragraph which is on… I guess which is on the paragraph that's up on the screen right now.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

We talked earlier about not really weighing in on whether we believed in opt-in or opt-out, but there's a phrase that says, about half way down that paragraph that talks about for discussing and documenting patients choice. If a provider has a responsibility for documenting patient choice, in essence that to me is another way of saying opt-in, because…

Deven McGraw – Center for Democracy & Technology – Director

Oh, okay.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Because if you're going to document something, you're really giving the patient the ultimate right to decide whether in or out. And I'm a little concerned that we were mixing messages here.

Deven McGraw – Center for Democracy & Technology – Director

Okay. No, that's a fair point. I think we can re-word that so that it's documenting… well yeah, I'm having trouble figuring it out on the fly, but I totally see your point.

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

But you could document the patient's decision to opt-out, couldn't you, and then explain that you've worked your way through that with the patient, they understand what they're giving up?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

When we do an opt-out, because that's the direction we're going with our HIE is that, unless the patient comes up and says, I don't want to be in your HIE, they're going to be in the HIE.

Deven McGraw – Center for Democracy & Technology – Director

Right, there's no documentation required.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Right. If you engage the patient in a discussion and say, well would you like to be in or out, you're really saying, unless you say you want to be in, you're out… so in essence, it sort of acts as a de facto opt-in process.

Paul Egerman – Businessman/Entrepreneur

And this is Paul. One… I'm trying to understand the question and make sure we're answering it. But, this relates to an NVE or, as we used to call them, an intermediary; and it occurs to me that the intermediary might be dealing with some providers that have like an opt-in approach and some providers that have an opt-out approach, so they have both occurring and when that happens, how do they validate that things are done correctly.

Deven McGraw – Center for Democracy & Technology – Director

I mean, I guess… this would be the… this would be a set of choice policies that would be implemented by the NVE. So, I don't know too many single NVEs that are having both opt-in and opt-out choices.

Paul Egerman – Businessman/Entrepreneur

So, to participate in a particular intermediary, the provider has to go along with the approach to meaningful choice that the intermediary decides on?

Deven McGraw – Center for Democracy & Technology – Director

Yes. Yes.

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

The provider has a choice of which NVE to use.

Deven McGraw – Center for Democracy & Technology – Director

Well, that's absolutely right.

M

Or, if there's only one NVE in the particular communities region, they may be forced, if they want to participate with the NVE, they're going to have to deal with the policies of the NVE.

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

Yeah, that's true.

Deven McGraw – Center for Democracy & Technology – Director

Well right, unless they want to use direct protocols, assuming they can do that without an NVE of some sort in the middle.

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

It seems to me though…this is Dixie… that in most cases… maybe this comes right back to our discussions about control, but in most cases it seems like the provider would be the one that would be giving a patient meaningful choice. In most cases, I don't think the patient would have any knowledge of an NVE.

Micky Tripathi – Massachusetts eHealth Collaborative

Well, here's what… let me just give you, by example, what we do in our region with our HIE. We actually created a separate notice of privacy practices for the HIE. It becomes an addendum to each provider's individual notice, and we give that to each patient and the patient can read through it, and it says, you have the right to opt-out if you do not want to participate in this exchange and if you do, you don't… none of the providers that are part of this exchange will exchange your information. Then it's up to the patient to say, "I would like to opt-out."

Deven McGraw – Center for Democracy & Technology – Director

Right.

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

Hmm.

Deven McGraw – Center for Democracy & Technology – Director

Right. Right.

Wes Rishel – Gartner, Incorporated

This is Wes.

Deven McGraw – Center for Democracy & Technology – Director

Hi Wes.

Wes Rishel – Gartner, Incorporated

I'd like to… sorry I missed the roll call.

Deven McGraw – Center for Democracy & Technology – Director

Okay. I'll get you. I've got you down.

Wes Rishel – Gartner, Incorporated

I'd like to suggest that this framework will be in place at a time when not all NVEs are regional, so that the notion of physician choice among NVEs or HIEs is a bit broader than we've been thinking of it in the past.

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

Well that's… yeah.

Deven McGraw – Center for Democracy & Technology – Director

So what do you think that suggests for…

Wes Rishel – Gartner, Incorporated

Well, it suggests that there's more… that any concern about a physician being forced into specific consent model by not having a choice of HIE is diminished.

Deven McGraw – Center for Democracy & Technology – Director

Got it. So John, I think we can do some wordsmithing on the documentation issue, so that it doesn't appear as though some sort of documentation would always necessarily be required.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Okay.

Deven McGraw – Center for Democracy & Technology – Director

Because I can see how in opt-out models, if the patient says nothing, or doesn't seek to opt-out, there's really nothing to document. So…

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

Although it is still required, or we're still recommending that the patients not being surprised by the fact that the data's being exchanged so that at a minimum, there's some attention… call the patients attention to the policies for sharing that they are being defaulted into.

Deven McGraw – Center for Democracy & Technology – Director

So, that's right, I mean, there are conditions for meaningful choice which we reiterate in this response, include full transparency, education and opportunity to make in advance. And then, whether the default is in or out, was less important to us, and the RFI picks up on that concept. And there are other parts of the RFI which we'll get to that talk about notice.

Kathryn Marchesini – Office of the National Coordinator

Deven, this is Kathryn Marchesini with ONC. I just had a quick question. In the situation where I guess the opt-out is not documented, how are things currently verified, I mean, for example, if the patient chose to opt-out how is that tracked?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Can I tell you how at least, give you an example how we track it?

Kathryn Marchesini – Office of the National Coordinator

Sure, that would be great.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Our HIE by default you're in unless you opt-out, so, when a patient comes in any facility, part of the registration is that we would actually send a registration flag at the point they decided to opt-out of our HIE, and that's all done electronically, so, until we see a flag that says that the patient has opted out, you're considered to be opted in. However, having said that though, we make sure that the patients actually seen a notice, the notice to participate in the HIE, because nobody can give data within the HIE until somebody has actually registered for treatment. So therefore, as part of the registration process, if we ensure that we are providing that notice with the documentation of the HIE and what's involved, as well as during the registration process allowing the person to opt-out and that being electronically sent to

the HIE, we can ensure that the only time the patient's information is actually communicated is after registration, at which time the patient would have had the opportunity to have opted out.

Paul Egerman – Businessman/Entrepreneur

This is Paul. That was a helpful discussion from the provider side; but remember, this question relates to the intermediary.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Well, the intermediary being, we all set up the intermediary because there are nine hospitals… or nine health systems that did this. So, we all decided how to make this all work. So…

Paul Egerman – Businessman/Entrepreneur

What I was about to say is, depending on how the intermediary is structured, if it's like the intermediary is a centralized data model for example, if there's an opt-out situation, the patient's data just might not be available to the intermediary at all. In other words, it may never have been sent from the provider to the intermediary. And in some federated models, it could very well be that if the patient has decided to opt out, that there's not what I would call… loosely call a pointer. In other words, that basically that the intermediary doesn't even know that the data is there or that it exists.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

In our particular case, we do… we had the HIE as a business associate of every provider and we actually store all the data within the HIE that's going to be communicated and if you opt-out, we just don't make the data available.

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

John, this is Joy. To me what you described is a documentation; it's an electronic documentation, it's not a separate signed document though so…

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Well, we actually get the patient to sign something as well if they opt-out and then it's forwarded in the medical record.

Deven McGraw – Center for Democracy & Technology – Director

But certainly an NVE can take whatever steps it thinks it needs to do in order to have appropriate documentation. But it's also true that if you decide on a meaningful opt-out model and the purposes for which you're exchanging data do not otherwise require consent or authorization from the patient under Federal or State law, there isn't a legal need for documentation.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

You're correct.

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

You know… this is Dixie again… thinking about what Wes says and I'm sure that that's true, there will be multiple NVEs, but at least in my mind, a provider would be the one to decide which NVEs to use, not the individual.

Deven McGraw – Center for Democracy & Technology – Director

That's correct.

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

And in that context, I'm not sure an NVE could ensure that individuals are provided a meaningful choice, because a meaningful choice would have to include a choice between more than those that the provider may have selected, one or more.

Deven McGraw – Center for Democracy & Technology – Director

Except that's not really not the definition… it's meaningful choice as to the terms of information sharing in that particular NVE. It's not meaningful writ large to the whole potential universe.

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

Right.

Paul Egerman – Businessman/Entrepreneur

And this is Paul, just a question. If we say providers can choose the NVE, does that mean that the patient's data could be in more than one intermediary?

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

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Businessman/Entrepreneur

That doesn't make a whole lot of sense…(indiscernible) case there.

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

Yeah.

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

Yeah. This is David. I think one thing that we're seeing more and more of is the notion that opt-in and opt-out are in and of themselves inadequate descriptors of real world policies and that you usually have some mixture of the two where you might, for example, have an opt-out of a locator service but an opt-in to actual specific provider access; which is one of the things I like about our meaningful choice rubric and even though it's vague, it allows for the fact that there is more than one way to do this…

Deven McGraw – Center for Democracy & Technology – Director

Yes.

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

… depending upon the scope and scale and relationships involved. As long as the patient has the ability to eventually decide that they do or don't want to participate, I think we've got the right spirit.

Deven McGraw – Center for Democracy & Technology – Director

I agree. Any other thoughts about either the language that we've teed up for you or additional considerations? We have the advantage of having gone through this issue pretty thoroughly one summer not too long ago, which is good.

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

One question, Deven, that jumped out at me a couple of times… this is David again… a couple of times in reading this is the use of the word choice instead of consent.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

Are we comfortable about that?

Deven McGraw – Center for Democracy & Technology – Director

I could go either way. I personally use the them interchangeably, which is why they are interchangeable in the language, but if people are more comfortable sticking to one term consistently and prefer consent over choice, I'm fine with that.

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

Well meaningful choice obviously works well as a phrase, but there was just one place where it didn't sound right; it was something about the patient has… oh, I can't find it right now, but, you're not using the words to mean something different, that was really my question.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I certainly am not.

Wes Rishel – Gartner, Incorporated

I think we… I mean just as a… just because I was taught this, I think we ought to be consistent in our use of a word, not… it's my inner Mr. Monk coming out… and somehow I just have the impression that consent is more specific to what we have in mind and choice is broader, so I would… Mr. Monk would argue for using the word consent.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

And I found the one sentence… this is David again, the one sentence where it didn't read right to me, and it's, I think on the previous slide, the Tiger Team agrees that choice should not be required when an NVE is facilitating secure directed exchange. This doesn't read right, it's like, what do you mean I don't have choice… you know, I picked my doctor. So, use of consent in that space is much clearer, I think, so maybe you could try it… I mean meaningful choice, meaningful consent… yeah, I guess meaningful consent works okay.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, it does…

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

I think that's much more accurate.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, let's use consent, we can always drop a footnote saying that we believe that the terms choice and consent mean the same thing and we believe consent works better, just in case.

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

Good. Thanks.

Deven McGraw – Center for Democracy & Technology – Director

Anything else before we move to the next topic? Okay. Authentication. This is condition S2: An NVE must only facilitate electronic health information exchange for parties it has authenticated and authorized, either directly or indirectly. And here's the series of questions that follow: "What is the most appropriate level of assurance that an NVE should look to achieve in directly authenticating and authorizing a party for which it facilitates electronic exchange?" Question 25: "Would an indirect approach to satisfy this CTE reduce the potential trust that an NVE could provide? More specifically, should we consider proposing specific requirements that would need to be met in order for indirect authentication and authorization processes to be implemented consistently across NVEs?" Question 26: "With respect to

the CTE as well as others, should we consider applying the "flow down" concept; that is, should we impose requirements on NVEs to enforce upon the parties for which they facilitate electronic exchange in order to ensure greater consistency and/or compliance with the requirement specified in some CTEs?" Okay, just checking to see if I got all the questions.

The indirect approach, as I understand it, and those of you have also read through this RFI can do a gut check on this for me, is essentially if an NVE authenticates an entity, the expectation is that the entity would then be responsible for authenticating its individual users, which is the indirect way that an NVE authenticates an individual person user of its network. That was my understanding of what was meant by indirect, but folks can certainly chime-in if they think I'm way off on this or there's more to it.

Wes Rishel – Gartner, Incorporated

This is Wes. I think you are right and it's worth noting that it doesn't require indirect, it simply permits it. I think there are other cases of indirect in the sense that an NVE might have an arrangement with another NVE where the second NVE is responsible for authenticating the users and the second NVE might have delegated that to its users, its organizational members.

Deven McGraw – Center for Democracy & Technology – Director

Right.

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

This is Dixie. I want to bring up a point that I actually brought up at our privacy and security workgroup this morning as well, this particular one gets its terminology and its concepts a bit muddled and if you read the full paragraph that goes with it, you realize it really… they're mixing apples and oranges kind of here, or maybe two things that are a little closer, maybe lemons and oranges. But, basically, when you get a digital certificate you need, ahead of time, not in real-time, offline you have to identity-proof the entity, whether it's an organization or a person, make sure that they are who they claim to be, before you even give them a digital certificate, and you also, ahead of time, when you set up a system, you authorize them with certain privileges and accesses.

Then, all that's done ahead of time, and then in real-time, you authenticate an identity. So, I log in, I say I'm Dixie Baker, the system checks to see that I'm… you know, Dixie B is in the system, and then looks at my authentication proof and says, yes indeed, this looks like that's who it is and then they do access mediation to make sure that I can do, checking against those authorizations, I can do what I'm trying to do. And this particular CTE gets those processes mixed up. Because if you really in truth, you want them to do identity proofing ahead of time and you want them to do authorization ahead of time, and you want them to do authentication and access control in real-time; but they've put it all in one thing, it seems and the whole identity proofing sort of gets loss, even though when you read their words, it's there. So, I think this basic condition has… the way it's stated has problems so that even effects what directly and indirectly mean. Like, who do I have to get my digital certificate from? So, they've mixed concepts here.

Wes Rishel – Gartner, Incorporated

Yeah, I remember thinking about that as I read the document and wishing they had at least defined authorization, so that perhaps they intended to somehow blend the two concepts in order to… of identity proofing and assigning privileges, but, I would have to agree that it's likely to be read differently by different readers as it exists now.

Deven McGraw – Center for Democracy & Technology – Director

Hmm.

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

So, this is Joy. Could you suggest alternate language then?

Wes Rishel – Gartner, Incorporated

Ohhhhh.

Deven McGraw – Center for Democracy & Technology – Director

Joy is wondering if alternate language would be suggested. I'm wondering if…

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

I can give you alternate language that we came up with this morning.

Deven McGraw – Center for Democracy & Technology – Director

Well, that would be good. The other thing I was going to suggest is that we try to reflect in our answers the distinction that we would make and what we would ask NVEs to be responsible for.

Wes Rishel – Gartner, Incorporated

I would suggest that we take the language that Dixie proposes and have a discussion of that, if the schedule permits the deferral of this topic that long.

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

But wait… and I should say to Deven that we weren't actually addressing these questions. The last question is would you add any CTEs, so that's how we…

Deven McGraw – Center for Democracy & Technology – Director

Ahh.

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

This is David. I mean, I totally agree that this is not precise use of the technical language of security, nor is it use of the language consistent with other Federal uses of… when they're discussing this subject; however, it seems that the spirit of the question is pretty clear and from a policy point of view, we ought to weigh in on the spirit of the question. For example, is there a minimum appropriate level of assurance that should be required before someone can participate in data sharing using NVEs. I mean, we've had debates about that in many contexts for a long time, but that's still an important question.

M

Can you say that question again?

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

Is there a minimum level of assurance of the user's identity? In other words, NIST has defined all the different levels of assurance and you can range from basically nothing all the way up to a biometric, certificate in hand, military grade user level of assurance. And, what I think is being asked here, just broadly is, does the notion of an NVE certification, possession that you are in fact an NVE, does that mean you must guarantee a minimum level of assurance for everyone who participates in your system, and I think that's still a really valid question, even though the language here is somewhat muddled.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, you know, so I will say that we put together… I personally didn't see the mixing of the lemons and oranges that our security experts saw, so, in pulling together some potential straw man responses based on some of the policy recommendations that we had previously teed up, that they may not look precisely right, but may get to the spirit issue. But, we should take a look at them and then see if it's possible to address the questions that have been assigned to us without a deeper consideration of a distinction between identity proofing and authentication.

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

That sounds fine to me.

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

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Does that sound okay? Yeah…

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

Yes. I agree.

Deven McGraw – Center for Democracy & Technology – Director

We do have one more call and we have lots of topics, so it's not like we couldn't move on and come back.

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

Yeah, I agree.

Deven McGraw – Center for Democracy & Technology – Director

So what we tried to pull together here was to say that consistent with previous recommendations of the Tiger Team and Health IT Policy Committee, NVEs should have a high degree of assurance in authenticating parties for which… okay, now we have a pronoun problem… which they facilitate electronic exchange. CTEs should allow for authentication of participating entities and then leave to each entity the responsibility of authenticating their individual users, which is certainly consistent with our previous recommendations regarding entity level digital certificates. NVEs may, but should not be required to, set additional policies for individual user authentication such as requiring more than user name and password for remote access. This was also a recommendation that we had previously made. And then, NVEs that do allow for individuals to access information directly from the NVE, must authenticate individuals and again, this was one where we considered whether there might be different models of NVE where entity level authentication might actually not make sense. So, I don't know if any of them continue to make sense, given that we didn't really pick up on the distinction between identity proofing and authentication, but, is there something we can do with these?

Wes Rishel – Gartner, Incorporated

I think it makes perfect sense as applied to authorization.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

To authentication.

Wes Rishel – Gartner, Incorporated

I'm sorry, as applied to authentication.

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

Authentication.

Wes Rishel – Gartner, Incorporated

Yeah, authentication as it said.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Wes Rishel – Gartner, Incorporated

I think as you get through… you can probably use almost the same language for identity proofing.

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

Yeah.

Wes Rishel – Gartner, Incorporated

I think it gets really to be a mess around authorization though.

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

Yeah, yeah, I totally agree. I don't know what high degree means though. High degree to me, if we put high degree to Dixie Baker, that means absolutely passwords are not adequate.

Deven McGraw – Center for Democracy & Technology – Director

Right.

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

Especially passwords that's the name of your dog… you know, that doesn't say anything.

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

Yeah, I hear this, but I think we struggle Dixie with landing on a NIST level when we had this discussion in the committee and ultimately defaulted to… especially in our digital certificate conversation, where you wanted a high degree of assurance that the entity is who they say they are. It was not… we could not sort of get ourselves to agree on the number for NIST because that sort of translated into certain policy decisions about what would need to be presented in order to authenticate and we couldn't get consensus on that. That's where we landed.

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

It also seems to me that it should take into consideration whether you're authenticating an organization or an individual, because the risk level is much different.

Deven McGraw – Center for Democracy & Technology – Director

Right.

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

But the general… this is David again… coming back to the general spirit of things, I think this captures what we've said before, which is, we do think it's appropriate for there to be organization based layering, so that the organization is responsible for authenticating and authorizing and identity-proofing the individuals, as well as direct individual access, which means that the NVE is responsible for doing all those things. Those both make sense and I agree, we weren't able to decide on a specific level; I think debates that we've had outside envision that you could conceivably have a trust network where there are different levels of trust, depending upon who you're connecting to, that is technically possible. Whether you can get a minimum agreement that everyone in the whole country will agree to for exchange of patient data is, boy that would be nice, but I don't know how you get there, short of an iron-clad rule and that's a politically tough call.

Deven McGraw – Center for Democracy & Technology – Director

Right, and not even something that can be imposed through this governance vehicle, which is largely going to be voluntary, unless it gets adopted and imposed as a mandatory condition in some circumstances. So…

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

There is another NVE notion, or one of the CTEs, is participation in Federal Bridge, and if you do that, that by default, pulls in all sorts of requirements that go beyond what we're talking about here.

Deven McGraw – Center for Democracy & Technology – Director

Well, and you know, that's the next one up on our list. Well, here's what I'm going to suggest. I'm going to suggest we leave these for now, but if folks want to work offline to wordsmith them a bit, we can do that and take up any wording changes either in an online way or take a few minutes on the next call to do that. Does that sound like a workable plan?

M
Agreed.

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

Deven McGraw – Center for Democracy & Technology – Director
Okay, so here is what we said about digital certificates. So, the condition is that, and this is an interoperability condition, that's why it starts with an I instead of an S, an NVE must follow required standards for establishing and discovering digital certificates. And the question assigned to us is "Should the CTE require all participants engaged in planned electronic exchange, to obtain an organizational or group digital certificate consistent with the policies of the Federal Bridge?" And here is what we said in our straw man response, based on recommendations that we previously came up with, is that we believe that all certificates used in NwHIN exchanges must meet Federal Bridge standards and be issued by a certificate authority or one of its authorized resellers that is a member of the Federal PKI framework.

And then the second bullet point, which is not exactly on point with our previous recommendations, but reflects the fact that there were a lot of conversations that took place after our recommendation about whether, in fact, there were… it would be possible to get a Federal Bridge certificate issued at the organizational level; which I understand is still being worked out, although heading in a positive direction from last I was told. So, we just added a straw response that said that this could be phased in, and we certainly can caveat it and say, phased in if in fact Federal Bridge certificates are not available at an organizational level… or not widely available at an organizational level. What do folks think about this?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics
This is David. Just a clarification question, in point number one do you mean NVE instead of NwHIN exchange?

Deven McGraw – Center for Democracy & Technology – Director
I think we were talking about NwHIN overall, so that certificates issued to NVEs or certificates… hmm, hang on a second.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics
I think you mean NVEs.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics
What does the N in NVE mean though?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics
Well, NVE is an NwHIN Validated Entity.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics
So, I guess you could probably use them interchangeably, I think, in this case.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics
Well, but my point is NwHIN exchange is, currently that means to most people, the query model…

Deven McGraw – Center for Democracy & Technology – Director
Oh, right, no, you're right. I don't (indiscernible) the letter exchange.

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

No, that's not a capital E, but it still has an issue. What I thought you were going to David is that all certificates used in NwHIN exchanges would go down to the individual level, and I don't think that was our recommendation at all. It was that…

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

It wasn't.

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

… organization level.

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

I agree, we need to stick with organization and I just want to say that I'm just saying that everywhere else we've been talking about NVEs and this shift language here implies that you're somehow singling out a subset of NVEs and I don't think we're doing that.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, good point.

Paul Egerman – Businessman/Entrepreneur

David and Deven, this is Paul. The question is… the questions say all participants, so it says all participants; it's not limited to NVEs.

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

Yeah, it should be all participant organizations.

M

Yeah, so, I think… because of the way that I view it, to me when I saw all participants, I thought that meant all participant organizations, although your comment is a good one Dixie, if I had viewed it from a different perspective, I might have thought it meant individuals.

M

Could we say something like all certificates used to exchange information through or among NVEs must meet Federal Bridge standards?

Wes Rishel – Gartner, Incorporated

Well, I think that's a good thing to say, but I think it's also good to, as Deven said, drop a footnote that says we're specifically talking about organizations here. I mean, it's probably an accidental ambiguity as opposed to specific intent and it's sort of pointing out the ambiguity.

M

I did read it as participant organizations, I think that's what they meant.

Wes Rishel – Gartner, Incorporated

I do too, but it doesn't hurt to… given the sensitivity of this particular issue, it doesn't hurt to redundantly repeat ourselves.

M

But the important point I was trying to make is, it's all participants, it's not just NVEs, it's the organizations that interact with the NVE also have to have these digital certificates or whatever certificate it is that we're going to answer with.

Deven McGraw – Center for Democracy & Technology – Director

Right. So since the criteria though, I like John's language because these criteria apply at the NVE level, so what you're saying is NVEs have to make sure that their participants have digital certificates, organizational digital certificates that are certified or cross-certified to the Federal Bridge.

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

Yeah, we could actually insert organizational before certificates and then change the NVE and we'd have it. All organizational certificates used by the NVE must meet…

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

Yeah, now, do we really want to say that, are we still comfortable with that, given the difficulties that… I guess the phase in is our allowance for the fact that at the moment you can't get an organizational certificate.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, that was my idea.

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

They do meet Federal standards right now, which is kind of a… that part that says meet Federal Bridge standards, is kind of a moving target right now.

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

Yeah, and I don't think… remember we put two constraints; one was that it meets the Federal Bridge… one is that it's organizational and the second that it has to be a healthcare organization.

Wes Rishel – Gartner, Incorporated

Right, and the question was, if I remember the question correctly, it said consistent with Federal Bridge, which is not quite the same as saying Federal Bridge.

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

Yeah, that's why we changed it to consistent with is because of that moving target.

Deven McGraw – Center for Democracy & Technology – Director

Ah, okay.

M

I don't know if you noticed that Deven, but…

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

Yeah, that introduces yet another level of ambiguity, although I like it actually.

Wes Rishel – Gartner, Incorporated

Well, I think…

M

But I thought we're consistent I sort of thought.

M

Well, something that's pretty much, kind of like, almost exactly the same, but maybe not the same.

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

I would bet you there are Federal partners who wouldn't count that.

M

Pardon me?

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

This is David. I'm guessing that there are Federal partners who would say, we can't technically connect to somebody who's merely consistent with…

M

Well that could be, but again we're not talking about the Federal partners in this context, we're talking about a governance RFI and the way I'm reading this is, you know, they're looking for organizational certificates that are consistent with Federal… maybe I'm reading too much into that word…

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

I think what we have here Paul, it says must meet Federal Bridge standards and right now, Federal Bridge standards are not an absolute because they don't have organizational certificates, but ultimately… so Federal Bridge accepts that exception if you will.

Wes Rishel – Gartner, Incorporated

Dixie, this is Wes, and point of information here. For the certificates that are issued consistent with the Federal Bridge policies, don't those policies enumerate a chain of connection of the enumerators of the… I'm saying this very badly, but, don't the policies actually imply very directly that the only people who can issue these certificates are people that are authorized for the Federal Bridge…

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

Yup.

Wes Rishel – Gartner, Incorporated

All right, so I think that the… as a practical matter, the term consistent with should be regarded as under the policies of the Federal Bridge, because I think the policies are so clear and direct on this point that it's not likely that there's an evasion possible.

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

And our straw man response makes that totally unambiguous, it says it must be issued by a certificate authority.

M

Well, maybe I read too much into the word consistent, but that's what I saw and I do agree with what you're saying David, our straw man response is far stronger, in terms of what it says about the Federal Bridge and I was wondering if they used that sort of more lukewarm language mainly because of this problem that exists with organizational certificates and the Federal Bridge right now, that they're suggesting there might be some other alternative.

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

I think that consistent with is… makes it too subjective. I think we should suggest they use our language. I'll bet you they really didn't even know about the Federal Bridge issue.

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

Well, yeah, actually we do know about it, this is Joy. This is an issue that we continue to research, it is really very much more complicated than you would ever want it to be. As I'm looking at this, I think that it might be best to postpone this discussion a little bit so we can put together some more concrete information for you on this, to make it a more fruitful discussion. For example, I think that when… now that I'm looking at this really carefully, that a certificate authority that is a member of the Federal PKI framework, I think they use the term Federal PKI framework to mean only Federal members…

Deven McGraw – Center for Democracy & Technology – Director

Oh.

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

Um, yeah.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

So, why don't we take this one, we will make note of the comments that we've received to date on this, and I think we should take this one and give you a little bit more background information. Would that be helpful?

M

Yes, that would be.

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

Yup.

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

The Federal Bridge does have a specification for non-Federal members…

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

Exact… well, it has… I don't know that they call them members, they call them non-Federal entities.

Paul Egerman – Businessman/Entrepreneur

So what we're going to do with this is, we're going to get some information before we continue discussion of this question.

Wes Rishel – Gartner, Incorporated

Right.

Paul Egerman – Businessman/Entrepreneur

Which is actually consistent with the way we've handled these discussions in the past.

Wes Rishel – Gartner, Incorporated

We may be comparing California oranges to Florida lemons here.

(laughter)

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

I just want some lemonade.

(laughter)

Deven McGraw – Center for Democracy & Technology – Director

All right, then we'll resolve that one when we get more information. And we'll move on to encryption. And this condition, which is safeguard #4, proposes that an NVE must only exchange encrypted individually identifiable health information. And then the question that we've been asked to address is, "Should there be any exceptions to this CTE and if so, please describe them?" And based on what we have said in previous recommendations, here's the straw man response we developed for you: Tiger Team supports a requirement that NVEs encrypt data in motion or exchange data that's already been encrypted I guess is something we might need to add there; given the frequency of data breaches, we recommend that NVEs also be required to encrypt data at rest. This is, of course, when they actually have data that they are collecting and retaining, which won't always be the case for most NVEs. We presume that both recommendations will be accomplished by the CTE that makes all addressable HIPAA Security Rule

implementations specifications required for NVEs. And this one is one that got assigned in priority to Dixie's group on the standard side; but we referenced it here.

M

So Deven, I don't understand. So are we answering this or is Dixie's group…

Deven McGraw – Center for Democracy & Technology – Director

We aren't answering this question, but it's closely related, or at least I thought it was, to another CTE which essentially makes all of the addressable implementation specifications of the HIPAA Security Rule mandatory. We have… been asked to...

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

You know, (indiscernible)… in our meeting this morning and then Walter noticed that the HIPAA requirement actually doesn't say, you must, even though it's addressable, it doesn't say you must encrypt all data or even all data sent across the network. It says you have to be able to encrypt data. And so, we concluded it is needed, but, they also noted that same… similar to what you did, and the only comment recommendation that we had was to make it the NVE must assure that all data are encrypted, to account for exactly what you mentioned.

Paul Egerman – Businessman/Entrepreneur

If we could just divide this up. What we're talking about is first, what you call data at motion, which is data that is being exchanged from point A to point B, perhaps through an intermediary, and saying it must always be encrypted. Let me just ask a question, because the question is, should there be any exceptions and my question is, suppose the data is being transferred not over a public network? So, for example, suppose the healthcare organizations in the same building as the NVE is located, do you still need to encrypt it if you're just sending it say over a local area network? I mean, you could… is that an exception?

M

I agree with Paul's point. That is an exception in my opinion.

Paul Egerman – Businessman/Entrepreneur

You can make the argument no, there's no exceptions because a lot of people who transmit data over local area networks also encrypt it, but that would be the only exception I could think of.

Judy Faulkner - EPIC Systems Corporation – Founder

Yeah, this is Judy, I agree with you Paul. That's a good exception.

Paul Egerman – Businessman/Entrepreneur

You think that is a good exception?

Judy Faulkner - EPIC Systems Corporation – Founder

Yeah, I do.

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

Plus they defined it, so that that would not be an NVE.

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

And it might be that it goes over an encrypted channel, so I think we generally regard encryption of the channel or encryption of the message to equivalent to encryption in motion. I would think the channel would be required to be encrypted, you wouldn't, even within an institution, you would not want to be sending stuff over a non-TLS protected channel.

M

Well, I'm not clear whether, I mean, a typical exception has been private lines or leased circuits where there's… no one sees the data, encrypted or not, except the correspondents. And…

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

Even those are protected.

M

But they're not encrypted.

M

They're not encrypted, right, but normally…

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

Most people would use a VPN, wouldn't they?

M

No, the people communicating over the Internet would use a VPN, people using private circuits…

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

I would think they would use a VPN, but maybe I'm wrong.

M

(Indiscernible)… using a VPN, your argument could be, well the VPN is going do its own encryption, so find the intermediary, why do I have to encrypt it a second time? Why do I have to encrypt…

Wes Rishel – Gartner, Incorporated

Well, I agree, there should be no need for double encryption, but, I think that this… the way I recall the original HIPAA language, it was pretty clear that it applied to shared networks, not just… not to all networks, and that's what I'm not seeing here.

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

Well then why would we worry about encryption at rest and things like that, I mean…

Wes Rishel – Gartner, Incorporated

To me, encryption at rest is a totally different issue.

Deven McGraw – Center for Democracy & Technology – Director

It is a different issue and we (indiscernible)… we were just trying to incorporate recommendations that we had made where we could and I'm happy not to mix the…

M

Yes, because I think we're mixing up two different interesting and possibly controversial issues. Encryption at rest has its own interesting little discussion about it. So, I'm just saying… the question is, is there an exception and I just say is a non-public network is a direct connection, a local area network or private line a reasonable exception to this rule.

M

I think it is.

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

I mean, there are two protocols that are currently being discussed for use in these NVEs, I think there will be additional protocols, but the two that are currently being discussed, exchange and direct, both use a secure channel, I mean, direct uses an encrypted message and exchange uses a secure channel; so even if you had a private line, it would be… an exchange message would go over encrypted channels, so,

it's a moot point for the two protocols that are under discussion. Maybe this is a protocol question and not an NVE question.

Deven McGraw – Center for Democracy & Technology – Director

Or maybe it's an issue of the condition, not necessarily being appropriately worded, so that it leads people to think that it's talking only about message encryption versus only using secure channels for transport… or secure channels or encrypted data… I mean maybe there's a way to wordsmith it so that it incorporates you can use one or the other, but you should be sending securely.

Wes Rishel – Gartner, Incorporated

And also, actually as I think about it, I kind of like the last thing you said David, where you said it should be a protocol question and not an encryption question. That could be an interesting response, because where this thing should all be heading is eventually to some certification process for these NVEs and you can certify whether or not they're doing things according to a certain protocol.

Judy Faulkner - EPIC Systems Corporation – Founder

I like that, because…if we start specifying all the technical ways to do it, we're going to mess it up probably.

M

Well, that's right.

Deven McGraw – Center for Democracy & Technology – Director

Hold on, I hear John trying to jump in.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

To Wes' point though, it's not even a protocol issue. If you have a dedicated line, you know, between facilities, then it's not a protocol, it's you've made a decision in a secure fashion to have a dedicated line, your line is secure because it's dedicated. And by example, I have dedicated lines running to facilities all over Western Pennsylvania.

Judy Faulkner - EPIC Systems Corporation – Founder

I think you're running into two different definitions of what protocol means; one is, you're talking about a technical protocol and I think we're talking about a philosophical protocol; this is the way it should be done. I mean, not specifying the way, but saying it should be safe rather than here's how it should be safe.

Wes Rishel – Gartner, Incorporated

Well, here's what I think. The most important comment we've had is that we should kick this downstairs to validation of NVEs, rather than create a flat requirement that, for example, crosses light transmission between buildings and things like that. So, I think we can… we must not take a stand that's any broader than HIPAA here.

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

I think that they… I think this one is completely covered by HIPAA and we should suggest it be removed; because if they have to comply with HIPAA, they're going to have to do that. If it's over an exposed network, they'll have…

M

So that's a good…

Judy Faulkner - EPIC Systems Corporation – Founder

I think that's a great idea.

M

I think that's a good, may be a good way to answer, so maybe we say, in accordance with HIPAA, any… or we would state HIPAA already requires that any communication over shared networks must be encrypted.

Deven McGraw – Center for Democracy & Technology – Director

Or it must be secure.

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

No it doesn't, but between its requirement to support encryption and its strong emphasis on risk management, you're going to have to encrypt it if it's over an exposed line.

Wes Rishel – Gartner, Incorporated

Yup.

M

Right.

Judy Faulkner - EPIC Systems Corporation – Founder

Yup.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Maybe we can get rid of the data at rest encryption.

Paul Egerman – Businessman/Entrepreneur

The data at rest is an answer to a different question.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, it's going John.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Thank you.

Paul Egerman – Businessman/Entrepreneur

And, but the question still is, should there be an exception?

Deven McGraw – Center for Democracy & Technology – Director

Well yeah, but we're basically taking issue with the question.

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

That's why I suggested that Paul, is that if we just say we suggest eliminating this condition because it's already covered by HIPAA, then when you do your HIPAA analysis, if it's over a private network, then you wouldn't encrypt it.

M

Right, I mean, just re-reading the language from the preamble, I think the… first of all, well, see they bring in the OCR breach notification guidelines.

Deven McGraw – Center for Democracy & Technology – Director

Which currently only list encryption, but could be expanded to list other types of security over time.

M

Right, but for most of the cases around the OCR guidelines involve lost media and encryption at rest rather than encryption in motion. The… I just think that a suggestion that the CTE will create confusion by the overlap with HIPAA and the breach notification requirements rather than… and should be removed, would be the better approach.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

Okay.

Deven McGraw – Center for Democracy & Technology – Director

I'm fine with that.

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

There's a consensus on that.

Deven McGraw – Center for Democracy & Technology – Director

All right, so now we're moving on to notice, and again, this is relevant to NVEs. The condition is "that an NVE must make publically available a notice of its data practices, describing why individually identifiable health information is collected, how it is used and to whom and for what reason it is disclosed. And as you'll see in the preamble, there's a discussion about how this notice isn't just about what you're permitted to collect, use and disclose, but it's supposed to be a notice about what you're actually doing with data. And the series of questions that are asked about this condition are the following: "Are there specific uses or actions about which we should consider explicitly requiring an NVE to be transparent?" "Would an NVE be able to accurately disclose all of the activities it may need to include in its notice or should some type of summarization be permitted?" "Should the CTE require that an NVE disclose its activities related to de-identified and aggregated data?" And the last question, "Should the CTE require that an NVE just post its notice on a website or should it be required to broadly disseminate the notice to the healthcare providers and others to which it provides electronic exchange services?"

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

No.

Deven McGraw – Center for Democracy & Technology – Director

Okay, here's the straw man response that we came up with that addresses most of the questions, maybe not quite all of them, but is again, built on the discussion that we had about transparency and notice, many, many months ago; where we said that entities involved in health information exchange which would include those that are NVEs, should adopt the full complement of fair information practices when handling identifiable information and should be required to be transparent with regard…typo there… to how they collect… we obviously will clear up the grammar on this… collect, use and disclose such information. Transparency of information exchange practices is a necessary component of establishing credibility with patients; in achieving greater openness and transparency, we need to balance the need to give patient's complete information, while at the same time providing it in a form that is manageable and easy for them to read and understand; keeping in mind that this notice is probably one that has to, and maybe it's not the same notice, but that has to be able to be given to participants in an NVE as well as ideally patients who will have some meaningful choice about whether or not their data is part of it in many circumstances.

So, consistent with our previous recommendations, we were suggesting the following, again, this is a straw man; that NVEs should provide a layered notice, short 1-2 page summary of information sharing policies and activities and the summary notice should indicate how to obtain more information and a more detailed notice should be readily available. Important that the notice be written not only in plain English, but also at the reading level of the average patient and presented in compliance with applicable laws with respect to language and disability. NVEs should be required to disclose in the notice how they use and

disclose information including their use and disclosure of de-identified data, their retention policies and procedures and their data security practices. Again, all of this is from previous recommendations that we made on notices, which actually were largely aimed at notice to patients, not necessarily providers.

Additional points that we made here for your consideration that in the interest of transparency and building consumer trust, NVEs should give notice about what they actually do rather than just what they're legally permitted to do with respect to the IIHI that they're responsible for exchanging, and they should be required to broadly disseminate their notices to providers and others with whom they exchange information, although Dixie just said "No," so… we'll clearly have a discussion on that. So, there's a lot of language here, it does focus more on patient than provider, it's based on some recommendations that we came up with previously. We'll clearly have to clean it up, but I'm interested in your thoughts on…

M

The language, it seems to me, doesn't address also this issue about de-identified and aggregate data.

Deven McGraw – Center for Democracy & Technology – Director

Well, it does, in part because you may remember that one of the recommendations that we made with respect to intermediaries was that they should disclose to their participants what they're doing with de-identified data. And that was a recommendation that got approved by the Policy Committee and moved forward to ONC. It's not one that got a lot of press attention, but it has been in there all along; so, I actually am pulling the letter… third party service organizations, that was our name for intermediaries, should be obligated to disclose in their business associate or service agreements with their customers, how they use and disclose information including without limitation, their use and disclosure of de-identified data.

M

So, okay. Let's start with Dixie's answer, "no." That was really, I suspect you were talking about like this notification disclosure thing Dixie, but why don't you explain what you meant when you said, "no." Dixie?

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

Yeah, I just think posting it is just fine, I think it's just kind of overkill to require them to provide… you know, broadly disseminate the notice. One of the things that we suggested in the Privacy and Security Workgroup that you might want to consider though, is that as these validation bodies and ONC publishes the NVEs that have been validated, they might want to include a pointer to their notice.

M

And so, if you don't mind then, we'll start there. So, you're saying, Dixie, just put it up on the internet and let's not have one of these things where you have to send something in the mail and people just see a privacy notice and they throw it away without reading it, because it's sort of a nuisance.

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

Yes.

M

Okay, so does anybody disagree with what Dixie just said?

Wes Rishel – Gartner, Incorporated

Well, I want to comment that I think this interacts strongly with the requirements to state what you actually do, rather than what you're permitted to do because saying that you have to say what you're actually doing implies frequent updates. And, I can argue both ways whether frequent updates means there should be something more active than simply changing the contents of a website or not, but…

Paul Egerman – Businessman/Entrepreneur

I think we have to consider the two together.

M

And that's a good issue because one of the reasons why when people update these things, it sort of like causes everybody to not bother to read it, is they just reissue like a five page privacy policy thing and you can't figure out what the hell is different and it's just a bunch of words. So maybe, a variation would be to say, you simply have to give an update that explains what you change from last time.

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

Or you could require that they notify electronically their subscribers and say there's been a change and point to their website.

Wes Rishel – Gartner, Incorporated

Right.

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

I just think this broad dissemination of these letters like they do today are just…

M

Well, that's right, but what I'm saying is not just that there's a change, but you have to describe what was changed.

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

Right, right.

M

Because otherwise you could never figure it out, you just have to re-read the damn thing and it's like you never understood it the first time and can't tell with the issues, as Wes is saying, if you're describing what you did. So the way a change would work is we've just started to sell data to ABC Corporation. That would be a change.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

This is John Houston, just a couple of comments. I mean, I guess this is at the NVE level that we're talking about these notices. I'm a little concerned that in the interest of transparency that we're simply talking about posting and I think there's a strong case to made that, as we did, was have some type of addendum to notices that at least can be available or posted in facilities so the patients understood what was going on. But I'm also concerned with the idea that, actual uses change constantly and my concern is that, as I think has been stated, that this is going to be sort of, how are you ever going to get out in front of every time something changes, changing your notices or your communications and I'm a little concerned that that's just going to get very burdensome.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I mean it could. The Federal Trade Commission recent report on consumer privacy actually I think has some good language about how to distinguish between the types of changes for which you need to re-notify people specifically versus those that are relatively minor and don't necessarily need to be broadcast to the world. I can be looking it up as we discuss and it's obviously a test that's something along the lines of, significant changes or ones that would change expectations about how data is used; maybe we go back to the patient core values…

M

Okay, so like we've got meaningful notice now in addition to meaningful choice.

Deven McGraw – Center for Democracy & Technology – Director

(Indiscernible)

M

Meaningful notice but meaningful choice for meaningful changes.

M

But you know…

Wes Rishel – Gartner, Incorporated

I think if we confined some language to talk about… to decide what's meaningful that's helpful, but, I think we need to look at this issue very carefully because, for example, if I'm already selling information to Dow Chemical, does it matter if I'm also selling it to a pharmacy company? I don't… I think that way lies madness to be honest. I am concerned about the discussion about the pointlessness of public notification. I think it's a lot like government transparency, it's not that everyone pays attention to those notices, it's that advocates do and make noise in the press and that's a good thing.

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

Yeah, that part is true.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

So who's the notice really intended… is it directed at the patient consumer?

Deven McGraw – Center for Democracy & Technology – Director

John, I think that's an excellent question because I think we… our straw man response sort of mixes things up a little bit, because we had previously focused on notices to patients but if you look at the preamble language, I think that what they're looking for is both notices to the participants in the NVE as well as to the general public, and, maybe there are sort of different things that we would ask for for different types of notice, although, probably overlap in substance in terms of what's actually happening with data. It might be presented differently to providers, for example. I'm sure that you're very aware of what's going on in your HIE because you helped develop it and set the policies.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Right…

Paul Egerman – Businessman/Entrepreneur

So, what about what Dixie suggested, which is that there has to be some sort of web-based or public notice of all this stuff that would be accessible to patients and that when there are changes with the NVE, at their option could send us like a snail mail letter or they could send an electronic letter that simply says there's been a change and either summarizes what the change is and/or points them to the website, tell them where the change is, so it's short and simple.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Then again I guess the other question is one of granularity. How, I mean, I think this could be an incredible burden, depending on how minor a change requires…

Paul Egerman – Businessman/Entrepreneur

Well that becomes also an answer to some of these questions about what can you summarize and categorize things. Right, in other words, if you're able to categorize things and say, well we sell aggregated data to pharmaceutical companies, then you probably don't have to list out every time you sell something, right?

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

Yeah, that makes sense to me.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Businessman/Entrepreneur

And so if you allow categorization, it's only if you add a new category.

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

And it's the fact that you're doing it as opposed to the fact that you're allowed to do it, which is, I think, more important than the fact that it's a summary versus actual contractual details. So, summarization of what you're actually doing, maybe quarterly at a minimum or something like that? Is it being that precise?

Paul Egerman – Businessman/Entrepreneur

Well, another way to do it would be to sort of say summarize it and that's going to be the criteria for notice, but, quarterly you are going to disclose the details of what you did the prior quarter.

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

Yeah, yeah.

Paul Egerman – Businessman/Entrepreneur

Then you'd say, we participated in a study on, I don't know, pediatric asthma….

Deven McGraw – Center for Democracy & Technology – Director

Although those notices are not usually in that level of detail, which you shouldn't have to change them on a quarterly basis.

Paul Egerman – Businessman/Entrepreneur

In other words, all you would do though is like publish what you did.

Deven McGraw – Center for Democracy & Technology – Director

Right, or say, generally that you shared data for research purposes. I mean, it's terrible at that summary level, you give people an opportunity to get more information, but then you'll have to change the notice every time you adopt a different protocol.

Wes Rishel – Gartner, Incorporated

Well, yeah, I think there's also the issue of pre-notification versus post-notification which is really what I thought Paul's suggestion was leading towards…

M

I would say pre-notification is a summary, post is just a list of what you actually did. It's not a required change of notice, it's just part of the transparency; here's what we did, which actually people always think that stuff is like negative, it could be positive, I'm a patient, I might be excited to learn that my data is being used for the following purposes…

M

That's true, but there is a lot more money in pointing out the negatives than there is the positives. The… I think that the issue you got at Paul was that it's really hard to know what you're going to actually do next week, much less next quarter, when a delay could slip it into the following quarter easily. It's much easier to know what you did last quarter, although even that's a bit difficult.

M

Well, in a large organization or a large network, you may find that it's… things sort of slip through and you've totally forgotten about it.

Deven McGraw – Center for Democracy & Technology – Director

I'm just realizing that we are just about out of time.

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

That's right, interesting discussion.

Deven McGraw – Center for Democracy & Technology – Director

We have 90 minutes for this call. We'll work offline to try to capture some of the comments that we had on this particular issue, but we'll start with it on the next call. And I'll also ask you to… and obviously we'll go back to things that we need more information on that Joy has promised to get us more information on. And we will endeavor to continue in this vein on our next call, but in the meantime, if folks want to read ahead…and send their thoughts around about particular issues that we're going to take on in future calls that might help us get through this a little bit quicker, I'd welcome it. We should go to public comment.

MacKenzie Robertson – Office of the National Coordinator

Okay operator, can you please open the line for public comment.

Alan Merritt – Altarum Institute

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

MacKenzie Robertson – Office of the National Coordinator

Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Be right back… thanks everybody, terrific conversation.

M

Thanks Deven, thanks Paul.

MacKenzie Robertson – Office of the National Coordinator

Are you still there?

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

Should we schedule a follow up call on the (indiscernible) issue?

Deven McGraw – Center for Democracy & Technology – Director

I thought we'd take it up on our next call Joy.

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

No, but I meant you and me?

Deven McGraw – Center for Democracy & Technology – Director

Oh, and Paul. Yeah, that would be a good idea, because I think we have our regular co-chair calls starting on Monday and Monday is a holiday.

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

Yeah, and so, if one is not scheduled, we will, okay?

Deven McGraw – Center for Democracy & Technology – Director

Okay, thank you.

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

Okay, bye.

Deven McGraw – Center for Democracy & Technology – Director

Bye.

Public Comment Received During the Meeting

1. I think the point is that there needs to be an opt in or opt out decision - not a "no consent" model - for situations where there is a repository etc. (i.e. where not just pushing info) yes, it is kind of forcing opt in unless perhaps the doctor gives info to the patient and if the patient does not opt out the doctor could attest to a lack of opt out - which is not the same as opting in
2. Consent, unless implied, is typically in writing. Choice may be more likely to be verbal, and not documented in writing. Thus, there may be some dissonance between the terms: Consent and Choice.