

Tiger Team
Draft Transcript
June 11, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you. Good morning, everybody, and welcome to the second privacy and security tiger team call. This is the federal advisory committee, so there will be opportunity at the end of the call for the public to make comments, and the transcript will appear on the ONC Web site. Just a reminder for workgroup members to please identify yourselves when speaking. Let me do a quick roll call. Deven McGraw?

Deven McGraw - Center for Democracy & Technology – Director

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Paul Egerman?

Paul Egerman – eScription – CEO

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Latanya Sweeney? Gayle Harrell?

Gayle Harrell – Florida – Former State Legislator

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Josh Lemieux for Carol Diamond?

Josh Lemieux – Markle Foundation – Director Personal Health Technology

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Judy Faulkner or Carl Dvorak? Dave McCallie? David Lansky?

David Lansky – Pacific Business Group on Health – President & CEO

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Dixie Baker?

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

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Micky Tripathi? Neil Calman? Rachel Block?

Rachel Block – New York eHealth Collaborative – Executive Director

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Christine Bechtel? Christine can't make it. John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Wes Rishel?

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

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Joy Pritts?

Deven McGraw - Center for Democracy & Technology – Director

Joy told me she was going to be maybe a little late.

Judy Sparrow – Office of the National Coordinator – Executive Director

That's right. Thank you. Did I leave anybody off?

Carl Dvorak – Epic Systems – EVP

Carl Dvorak joined.

Judy Sparrow – Office of the National Coordinator – Executive Director

Deven and Paul, over to you.

Paul Egerman – eScription – CEO

Thank you very much, Judy. It's Paul Egerman. I want to say good morning to the members of the team and good morning to the members of the public who may be listening to our call. We appreciate your interest in our discussions. To quickly review for everybody, this is the privacy and security tiger team that was organized at the request of David Blumenthal and Joy Pritts to try to get some momentum and make some significant decisions related to privacy and security really over the summer months because the number of funding, the number of grants were given to HIEs to health information exchange organizations, and it was hoped that we could get some policy guidelines in place prior to October, which is also when stage one of meaningful use occurs.

What is going on is we are—to remind everybody—sort of working on a parallel path. We have two paths, to concepts we're working on. One path is a framework document that Deven McGraw put together, and that's sort of like a top down approach that is sort of like doing the job correctly. The second path that we are on is we are examining the work that the NHIN Direct group is sort of doing very independently in terms of developing a pilot project, and we're examining interesting questions that are coming out of that work. And that gives us a way to sort of basically ground our activities to make sure we understand the impact of the policies that are creating.

We had a terrific discussion. Again, I want to thank absolutely everybody who is putting this much time on such short notice to this very important project. What we're doing is extremely exciting, so I want to thank you all.

The question that we started talking about yesterday related to the degree of PHI exposure. What we are going to do in the agenda today is we are hopefully going to continue to discuss that question and hopefully come to a point where we can answer that question, and then we're going to try to move on to two other questions that have come out of the NHIN Direct efforts. Then what we hope to do is turn our attention back to the frameworks document to see if we can use what we've learned from that discussion and to go ahead and create a framework.

Before we continue our discussion on the open question, which we're going to define again in a minute, does anybody have any comments or questions about the agenda? Terrific. So the open question that we have relates to the degree of PHI exposure with the idea being that if you – through an intermediary, so if you send a transaction, and there's an intermediary that doesn't see any PHI, then that's actually the best situation because you don't know anything, and the analogy that I gave yesterday was if you're standing by a highway, and you see an ambulance go by, well, that's interesting, but you don't know anything at all. And so that has nothing to do with PHI or privacy.

If, however, you see an ambulance go by and, on the outside of the ambulance, there's a sign that says John Doe on it, and that's the name of the patient that's in the ambulance, then you know something. And so now the issue is, what is the degree of PHI and what are the policies associated with it? And I'm wondering, Deven, if there's a way that you might be able to articulate the question to make sure that people understand what's the questions that we're asking.

Deven McGraw - Center for Democracy & Technology – Director

I think we had – you know, there are sort of a couple of endpoints to the discussion, which I think Paul started to point out. One is obviously we're probably most comfortable with the scenario where there is no exposure of an intermediary to any PHI. But in recognition of the fact that there is likely to be intermediaries that will, for what many of us would consider to be legitimate business reasons, need some exposure to PHI, whether they're checking on med accuracy or transferring to standard code sets or what have you. And there's likely a spectrum of that kind of exposure.

Number one, one of the things that we talked about is what constitutes an exposure and what doesn't. In other words, how do we take Paul's ambulance analogy and think about how that gets articulated in a policy. What do we mean when we say that exposure doesn't make us comfortable? And so the principle behind this is, I think, one that's rooted in collection, access, and use limitations, which is that there shouldn't be any greater access or disclosure of data than is necessary in order to accomplish a legitimate function that you're performing. So at one level, if all you're doing is transporting data like an ambulance, you ought not necessarily to need access to the content. Then you might go in gradations depending on what that level of functionality is.

And I think, in general, we're comfortable with this notion of, you know, where the principle says, access should be limited to the purpose necessary. But how does that then get articulated into some more specific policy that is then enforceable? I'm not sure, Paul, that I'm doing any better job of articulating the question, but I think what we want to do is come to the conclusion that, number one, accepting that the data exposure ought to be limited to what's necessary to facilitate the purpose for which the transaction is occurring, what are sort of the components that need to be added to that in order to facilitate trust.

Paul Egerman – eScription – CEO

Let me try to phrase it. I'd say, for the message handling activities, in other words, message transportation activity, what are the acceptable levels of PHI exposure through the intermediary, and what policy boundaries need to be established for that?

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

Paul, can I suggest an addition?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

Sure.

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

I think you want to or we may want to consider this in terms of ... of handling by intermediary or phrasing it in a different way of services provided by the intermediary, and we may say that there is an acceptable policy for intermediaries that don't have the need to see the data and a different ... policy for those that do need to see the data, and the policy could go to any one of the number of things, such as vetting of the organization or handling of the data or other things.

Paul Egerman – eScription – CEO

To your comments, one is, again, because we're on a public call, please be sure to identify yourself.

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

This is Wes.

Paul Egerman – eScription – CEO

It was Wes, so thank you very much, Wes. If I heard you right, I think that would be extremely useful. In other words, if we came up with a way of saying here are the groupings or categories for PHI exposure, and here are the groupings of policies that go with it, I suspect that would be a good way of doing things.

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

Paul, this is Dixie Baker. This morning, as I was getting up, something occurred to me, and I put it together in a PowerPoint and sent it to you guys this morning. But what occurred to me was that there's really a spectrum of exposure ranging from the case in which there is no intermediary. It just goes from point A to point B up to, and this is the part that I don't think we captured yesterday, and I think we should, is the temporal element where not only is it exposed in the middle, and they may manipulate it in the middle. But they may retain it in the middle so that not only, to use your ambulance analogy, you know, if that ambulance keeps all your health records and carries it around with it forever and ever. You know, that's increased risk.

So if you really, you know, once you have a chance to look at it, you'll see it goes all the way up to, you know, the case in which they actually, that intermediary would retain PHI and make it available to third parties. In fact, if you like, I'll tell you what I have in this, if you like. If not, I'll just stop there.

Paul Egerman – eScription – CEO

I thought what you wrote was actually very interesting. It corresponds with what Wes said. Why don't...?

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

...retaining....

Judy Sparrow – Office of the National Coordinator – Executive Director

Could we put that up on the screen so we could see it?

Paul Egerman – eScription – CEO

Yes. Is there any way you could e-mail it...?

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

I did e-mail it to you, Deven, and Joy.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Let me forward it to Judy, and is there anybody specifically at Altarum that we should forward it to?

Judy Sparrow – Office of the National Coordinator – Executive Director

I'll take care of that.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Gayle Harrell – Florida – Former State Legislator

This is Gayle. If we could put that up on the screen, you know, I have been thinking about the same thing. I think we need ... and go, A. I tend to think in little pockets of information and go A, B, C, and you have different sets of policies depending on the level of exposure and also retention. I was concerned about retention of data. And even if it's not retention of the data, you'd probably have some kind of an audit trail as to where it goes, which could also be indicating PHI.

Paul Egerman – eScription – CEO

Right.

Gayle Harrell – Florida – Former State Legislator

You know, if it's going to an abortion clinic, that's one thing. If it's going to an HIV center, that's another thing, and all of that relates to some PHI.

Paul Egerman – eScription – CEO

It's really an excellent point, Gayle, about the audit trail, really excellent point.

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

I agree.

Paul Egerman – eScription – CEO

Because, fundamentally, it's like you look at the example you gave, Gayle, yesterday where there was an issue of liability and possibly litigation. But what these intermediaries will be doing, which is an important best practice and something that the policy committee already recommended, is keeping some traceable logs so they sort of keep track of what transactions they receive, what date and times they receive them, and then what date and time they transmitted something out, and even what they transmitted out. That would be good practice. That means there is something retained.

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

There is something retained, even if they have no access to the PHI. There is information, you know, if you have the name, which they have to have some kind of identifier in order to move it to a location. They have the name of the location it's going. That in itself ... PHI.

Paul Egerman – eScription – CEO

Yes, that's an excellent point.

Deven McGraw - Center for Democracy & Technology – Director

I think it's helpful to see Dixie's models, but I also want to caution against us doing model specific policy because, by definition, that limits our statements to the universe of what we're able to think of on the call today versus, number one, specifically addressing what we think is likely and having a clear, overarching, limitation policy, which I think we're generally agreed to. Then secondly, looking at the likely exposure that could occur in an NHIN Direct situation, which is where we're trying to be in this particular set of conversations, and anticipating what exposure levels might be likely and specifically that there ought to be policies that limit the reuse of that data and retention.

Paul Egerman – eScription – CEO

Specifically, I agree with what you just said, Deven, because really for at least this part of the discussion, as it relates to what we're trying to do, we're really looking at the message handling function.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

We will be, later on, looking at some issues with, like, centralized HIOs where people do retain the data really for the purposes of people accessing the data, and so that that's a very interesting issue, and there are other risks associated with this, with that model. But this is really a discussion about message handling. We want to make sure we limit the discussion to that first because there'll be the opportunity to talk about the other models later.

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

But, Paul, this is Dixie again. I want to remind you that one of the four implementations did expose information and manipulate information and could have just as easily kept it, so it's not a far-fetched....

Deven McGraw - Center for Democracy & Technology – Director

No, it's definitely not, Dixie. I just want to make sure that we keep this discussion focused on the data exposure that comes with various forms of message handling versus thinking about higher level exchange models. That's all.

Paul Egerman – eScription – CEO

What just appeared on the screen is the concepts that Dixie is putting forward, and I'd just say, first, this is a great job, Dixie, and a great graphical presentation or visual presentation where she's showing on the left, an arrow from low to high risk, and then she's putting in various point-to-point exchange risk levels and activities. Looking this list and thinking also about what Wes said, this is sort of a very technical list. Another way one could do this, I suspect, would be to put it into categories of activities where you have like payload exposed and modified. That's really another way you could look at that would be data transformation because that's something that occurs a lot, and so in other words, rather than call it payload exposed and modified, I don't know if that would be an acceptable way of doing this. It'd be nicer if we could have a smaller number of categories and make it a little bit more functional as opposed to database. I don't know if you have a comment about that, Dixie, or if other people have a comment about that.

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

I think you could certainly use the word – if you wanted to avoid using the word payload, you could use PHI exposed. But I do think that exposure of PHI to examine versus exposure of it and modification of it are in fact two categories of risk.

Paul Egerman – eScription – CEO

Okay.

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

Paul, I want to say thanks, Dixie. I think this really extends what I was suggesting are really important ways of—

Paul Egerman – eScription – CEO

This is Wes?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

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

Yes, this is Wes. Right. We are going to have to come to grips with this challenge of how little or how much to group together our discussions of policy across this spectrum just in order to have a reasonable discussion process. But putting in front of us the notion that it is a spectrum, and we have to make that decision, I think, is a critical part of our deliberation, and the danger of being too broad in our categorization is that we begin to impute requirements on all entities of some time that constrain people's entry into the industry ... the danger of being too narrow ... never get anywhere.

Paul Egerman – eScription – CEO

You think, Wes, this is a good way to approach this?

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

I think, having in front of us a spectrum and then making a decision of how to group the elements on the spectrum together to discuss as policy issues is a great approach. I'm really glad that Dixie proposed it.

Paul Egerman – eScription – CEO

Are there other comments? Does anybody disagree? Should we proceed with this? Rachel, you've got real world experience. Is this the right way for us to be going about this?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Paul, can you hear me? I can speak too if Rachel is not there.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Micky, go ahead. We can hear you.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I think that spectrum is terrific, first off, so thank you to Dixie for that. I've just got a couple of questions that maybe are questions that not necessarily Dixie needs to answer, but that we, as a group, need to answer. One just small clarifying question is what does CE stand for?

Deven McGraw - Center for Democracy & Technology – Director

Covered entity.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Sorry?

Deven McGraw - Center for Democracy & Technology – Director

I think it's covered entity. Right, Dixie?

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

Right, yes.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Okay. Great. So then, I guess, as I'm working my way up the spectrum here, I get the syntax checking, no change, then syntax checking with change. I understand those. Then how do we define exposure when you're thinking of that, Dixie? For example, if syntax checking means that I have to open up the message, would the case of syntax checking with payload not exposed be the case where I had to open up the message to check the syntax, but the data elements in the payload were encrypted?

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

Exactly.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Okay.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Paul, this is Adam Greene with Office for Civil Rights.

Paul Egerman – eScription – CEO

Hello, Adam.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

There's just two things I wanted to clarify. There's been talk of payload versus PHI. One is that our list of identifiers includes dates, including date of service, which can complicate the question of whether or not a payload actually.... To go back to your ambulance ... don't know who is in there, but we know that the ambulance is treating someone on a particular date. That's potentially a PHI. So as we look at, you know, it's going to be an open question as to what extent these different exchanges expose dates of service inherently.

Paul Egerman – eScription – CEO

Yes.

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

But the date of service is only PHI if the name of the patient is exposed, right?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Right. So if you don't have a patient name, but you have a male was seen on January 1, 2008, that's considered identifiable.

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

Right, but you'd have to see the payload to get that information. What I was trying to capture, and this is Dixie Baker again. I was trying to capture the case in which they looked at the header to figure out where

to route it to, but they don't see any of the health information that's in it, that's in the message, so that's the concept. You know, the wording may be wrong, but that's what I was trying to capture.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Right.

Paul Egerman – eScription – CEO

What you're raising, Adam, if I'm hearing you right, you're raising the question, what is the minimum amount of data that constitutes PHI.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Right, and the fact that there may be minimal risk to the particular data, but it's still actually maybe PHI, which is relevant, as we look to these models, as to whether or not a business associate agreement may be required.

Paul Egerman – eScription – CEO

You've already defined that.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Right.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

In other words, that's not really a question we should be answering because you've already answered it.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Right, and similarly, encrypted information is generally considered to be PHI because it's a code that is derived from the underlying information, unless you fall under what's referred to as a statistical method where you actually have a statistician kind of certify that this information poses a little risk. Encrypted information, we shouldn't treat as being somehow safe harbored and now PHI.

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

But it is for the breach notification rule.

Deven McGraw - Center for Democracy & Technology – Director

But it does for that purpose.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

But it's considered PHI. It just doesn't require breach notification. If it wasn't, for example, PHI, you wouldn't even have to think about breach notification because it wasn't subject to HIPAA. So we said that is PHI, but if it's breached, you do not have to do any notification.

Paul Egerman – eScription – CEO

I'm trying to understand what you're saying. In your view, Adam, are we approaching this correctly by looking at these gradations, or are you sort of saying PHI is like being pregnant. You can't be a little bit pregnant. You can't be a little bit PHI.

Deven McGraw - Center for Democracy & Technology – Director

I also think he's saying that essentially defining this around PHI exposure may not be at the level that we want to deal with because PHI is actually, again, a small amount of information can still be PHI.

Paul Egerman – eScription – CEO

That's what ... this is the right way to go about it though because we're really looking at the activities.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Yes, I think this is the right way. It's just, you know, as far as trying to figure out risk levels, I guess the next step is going to be what policies we need to implement based on these risk levels. I'm just kind of trying to set the bar as to whether PHI has been exposed, which would trigger whether or not there's a business associate agreement. As you get to that next step, I want to make sure people understand that even though they may not be considering the payload to be exposed, it still may be PHI that requires a business associate agreement.

Paul Egerman – eScription – CEO

So your view would be you need a business associate agreement, even if you've got encrypted data?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

That would be if you have a statistician certify that that encryption is low risk.

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

If you use the standard AES encryption algorithm that was in the IFR, and you encrypt the data using PHI using AES, are you saying that it still would be considered by law and by your office as PHI?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Yes, that's our current position.

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

And you'd still require a business associate agreement?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Yes, unless the covered entity has gone to a statistician method. I don't know of any universal, statistical determination out there that says this encrypted data poses a potentially low risk under the privacy rule, so it's more like a covered entity. It would have to go and separately use a statistician on this.

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

The statistical method applies to deidentification.

Deven McGraw - Center for Democracy & Technology – Director

That's exactly what he's talking about, Dixie. In other words, if you turn it into de-identified data from under the statistical method, then you don't have PHI anymore. Otherwise it doesn't matter what kind of wrapper or hashing you do. It's still PHI.

Joy Pritts – ONC – Chief Privacy Officer

Yes, but whether you require a business associate depends on what the recipient is actually doing with the data. Is it acting as a business associate? There are rules about whether it's a conduit, and I don't know whether that would apply here. But before we get there, I think that we've kind of gone off on this....

Deven McGraw - Center for Democracy & Technology – Director

Yes, I agree.

Joy Pritts – ONC – Chief Privacy Officer

...a little bit, and I'd like to get back to the....

Paul Egerman – eScription – CEO

Yes.

Joy Pritts – ONC – Chief Privacy Officer

...before we jump ahead, get back to the original analysis, if we could.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Sorry to bring us too far off.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That gets us down into a level of detail that we may ultimately need to get to in terms of how we want to enforce how we think these particular policies can be enforced, and BA agreements is one piece of that, but we first have to clarify what we think the policies ought to be.

Paul Egerman – eScription – CEO

Correct.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Before we move on, can I just ask one more clarifying question on the...?

Paul Egerman – eScription – CEO

Sure.

Deven McGraw - Center for Democracy & Technology – Director

Only if you answer it as well.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Dixie can answer it.

Paul Egerman – eScription – CEO

Sorry to interrupt. I just want to ask everyone to say their names before they start talking.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I'm sorry. This is Micky Tripathi. I know this addresses higher levels of exchange that we're focused on directed levels of exchange, but again, just so we all understand or are on the same page on the spectrum. When we speak of covered entity, Dixie, who are you thinking of? Is that the intermediary when you say ... because it says covered entities and then third parties? I just want to make sure I understand who you're thinking of there.

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

You bring up a good point. We probably should avoid using terms like covered entity and PHI both because they relate specifically to HIPAA.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right.

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

I really was talking about the owner, if you will, of the data, the originator of the data, the sender of the data.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Okay, and then third parties is?

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

Like an HIO. No, the intermediary is the HIO. Like pharmaceutical companies like researchers.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Okay.

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

Like insurance companies for actuarial purposes. Anybody that you might, you know, sell or provide that information to.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right, so you've got a sender, and you've got a receiver. This is higher level, so....

Deven McGraw - Center for Democracy & Technology – Director

Yes, can we please not go there?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes. Got it. Thank you.

Paul Egerman – eScription – CEO

Let's return to Dixie's slides and look at this slide and say, well, are there any groupings of these activities that we say somehow belong together, and because they belong together, they represent a category of issues of policies that we might want to consider. If you look at the high risk one, the retain PHI and repository and make it available to third parties, it seems like that's almost like a category by itself. But are there other things here? She actually categorizes the bottom three, categorize the other three together. Are there any other things that people think are like natural categories that there are two or three of them that the policies probably really ought to be the same?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. It seems to me that there's a clear break line between the routing only and everything below and everything above because, with the routing only and everything below through just basic ... cache kind of things, you can verify that the message integrity has been preserved. No one has opened the message for any purpose versus everything above. They've opened the message for something.

Paul Egerman – eScription – CEO

Let's start there. Is there agreement to what Micky just said? Any disagreement?

Deven McGraw - Center for Democracy & Technology – Director

I'm not disagreeing. I want to take that one step further, which is to say that from a policy standpoint, there isn't a need for them to open the message, right? In terms of data, limited access to data whether it establishes a policy or a principle, there is no access to information in either the message or the actual content.

Rachel Block – New York eHealth Collaborative – Executive Director

Deven, this is Rachel....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

...within the....

Deven McGraw - Center for Democracy & Technology – Director

What?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Aside from whatever is in the header in the metadata.

Deven McGraw - Center for Democracy & Technology – Director

Well, actually I meant to get to message as well.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Okay.

Deven McGraw - Center for Democracy & Technology – Director

I didn't mean for that to be put aside. Rachel, you had a question?

Rachel Block – New York eHealth Collaborative – Executive Director

Yes, I'm trying to follow this. The lingo, quite honestly, is a bit dense even for somebody who does this for a living, but we'll have to revisit that when we try to actually publicly explain what we've concluded. I just wanted to clarify, though, your point, and I think you actually made this once before on a call, and I wanted to ask you about it because, let me just give you a sort of practical scenario that we're playing with here, and tell me if what you just said would preclude it or allow it.

We would like to envision that our RHIOs have access to medication history information from a variety of sources and with patient consent at the point of access to care that that RHIO could make an inquiry and combine the medication history information for that patient into one file, which would require, obviously, PHI to do that, and send that back to the requesting physician. How would what you just said affect that?

Deven McGraw - Center for Democracy & Technology – Director

I wouldn't want it to affect it at all because I wasn't thinking in that level of functionality for an intermediary. I think I was thinking about the sort of bucket at the bottom that just is from routing only down. So I was thinking, I mean, I wasn't trying to state policy that I thought would be universally applicable to any intermediary across the board because....

Rachel Block – New York eHealth Collaborative – Executive Director

Yes, that's what I wanted to clarify.

Deven McGraw - Center for Democracy & Technology – Director

Oh my goodness, no. It's highly unrealistic and arguably completely inadvisable from a function standpoint. I think what I'm trying to get at here is we could have a policy, for example, that just said, you need to limit your access to data to that which is necessary to perform the function. And when you do access data, we're going to put a set of policies around how you can handle it, and that may require some definition by us about whether acceptable functions to use with data and what are not and in terms of how

long you can retain it, etc., so that it's not completely a discretionary act on the part of the business entity in the middle.

But what I'm struggling with is ways that, I mean, one option is to limit the data collection in the first place. You can either apply the limitations at sort of what can do with it once you get it, or you can apply them at the front end say, from a technical standpoint, there are definitely ways to do this that limit that access to information that can be linked to a patient. Certainly that's preferable rather than attempting to, especially where that access isn't necessarily needed versus when it is.

Paul Egerman – eScription – CEO

Let me break in and make two comments. First of all, going back to what Rachel said, just a comment. I look at this point-to-point exchange risk levels, and I think Rachel put forward something that's not on the chart that really should be, which is sort of a function is to aggregate data from multiple sources and make it available. That's what I heard Rachel saying that is a function that the HIOs do. Did I get that? Did what I say there make sense, Rachel?

Rachel Block – New York eHealth Collaborative – Executive Director

Yes.

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

That's why it's....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

But I think that's the tough one.

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

That's what I intended the top two to be.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes.

Deven McGraw - Center for Democracy & Technology – Director

I think the third party piece, though, Dixie, is confusing to folks.

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

The top two are intended to be what Rachel described because, see the distinction between the two and then the third one?

Deven McGraw - Center for Democracy & Technology – Director

Yes, I get that but I still, you know, Paul, I want to let you finish your comment.

Paul Egerman – eScription – CEO

Yes. The other thing....

Deven McGraw - Center for Democracy & Technology – Director

We're straying into more robust areas of exchange that we--

Paul Egerman – eScription – CEO

I know.

Deven McGraw - Center for Democracy & Technology – Director

--deliberately left for later discussion.

Paul Egerman – eScription – CEO

That's correct, and so that was the other part of my comment is we are straying into the other areas. What I would say to do is sort of like, just as Micky is drawing a line, like routing and below and above, there's a line there.

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

Yes.

Paul Egerman – eScription – CEO

There's another line that we're going to – I think we really need to draw about some of these things about aggregating data, making data available because what we really are talking about is the message handling function, which is why I was also interrupting you a little bit, Deven, because when you're talking about limiting the amount of data available, in some sense, in the function that we're talking about, the provider doesn't have a lot of choice. For example, what the provider is doing is submitting a laboratory order or an e-prescribing order. The order is the order. They don't have any choice. They do e-prescribing....

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think I'm thinking of, you know, well, I'm not talking about what's in the content of the message. I'm talking more about what might need to be in the message....

Paul Egerman – eScription – CEO

Right, but what might need to be in the message is actually ... correctly, is going to be defined by the standards committee, right?

Deven McGraw - Center for Democracy & Technology – Director

No, we should set the policy about what we think ought to be an acceptable level of – I mean, I don't think we should let standards be driving what clearly should be a policy consideration.

Paul Egerman – eScription – CEO

What I'm simply saying is if you order a drug, e-prescribing standard says what the message is, and it's not like the physician has a choice. They order the drug. The physician doesn't know what goes out on the message. It just goes out.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That's payload, right?

Paul Egerman – eScription – CEO

Yes. That's the payload.

Deven McGraw - Center for Democracy & Technology – Director

I'm talking about header then.

Paul Egerman – eScription – CEO

It's the same thing. The physician doesn't have any choice. The issue is these things exist. Quest, SureScripts, they take the messages, and they do something with them. That's how it works. Micky and Rachel, tell me if I've got that right.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Certainly with existing networks that exist today, and I guess maybe some of that is in the dedicated network provided by third party category when you talk about SureScripts and labs. Yes, they define how that works, but if I'm understanding what Deven is saying is that this routing and below, that's sort of, you know, there's perhaps a minimal set of policy that is needed for that and below, and she's proposing that what is in the header is one of those considerations that is still an active consideration, even for the routing and below, which seems to me to be correct.

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

This is Wes. Can I add something?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes.

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

I think that we are hitting on an issue that is very, very relevant to the discussions that are going on in with NHIN Connect right now, and there are three broad categories of data under discussion. One is what we are happy to call the payload, which is the entire data that is being sent from one place to the other from one application to another wrapped up in a syntax and presumably encrypted too. The other end is that information, which is inescapably available to the intermediary just to route the message, so from Dr. Feel Good to the Betty Ford Clinic. That is, if you're going to use the domain name system, then arguably we have to assume that information is....

Then there's this middle thing that is called metadata, which is very similar to the legal concept of metadata, as it applies in discovery and so forth, which is data about the data that is also a part of the package. And that may or may not contain protected health information, but what we need to do is find a way that the questions that I answer can be stated in a way that all of the committee members are comfortable. They understand the question, therefore, can give an understandable answer, and specific enough to help out whoever is making technology decisions based on the policies downstream, whether we're talking immediately about indirect or longer about all kinds....

Paul Egerman – eScription – CEO

That's very helpful, Wes.

David Lansky – Pacific Business Group on Health – President & CEO

Paul, it's David Lansky. I was thinking along the same lines as Wes, and I was just translating it to a more functional rather than structural view of what are the HIEs or intermediaries allowed to do. In some sense, one outcome of our discussion may be prescriptive or restrictive to what an NHIN Direct model can be, and so what I'm thinking is, we've got something, which I'd call passive routing, for lack of a better word, which is really where Micky's line of the routing is on Dixie's chart. And I'm not sure that's a real thing, but conceptually it's a real thing. In other words, I'm not sure it's a real thing in the HIE world that is being built right now.

Then you've got what I'd call active routing, which is where someone has to look at the header and maybe make some changes or syntax in Dixie's chart. Maybe make some changes to that to successfully route to the message to a recipient. Then the third category, which is huge, which I'll just call it value

added in which there's some kind of manipulation of the payload or inspection of or manipulation of the payload, and that's the one obviously that is the most high risk and worrisome and policy complex.

I suspect, as soon as you cross that line into the third bucket, we've opened the entire can of worms of all the policy issues of audit, breach, retention, etc. that is a very robust policy framework that we're going to come to later in the call. Essentially, all of the rows of the policy framework have to be addressed once you've crossed into the third big bucket. If that's true, it sort of guides some of our work to say that maybe there's a class of policies, which is relatively compact that speaks to the active routing set of functions and applications. And maybe you could say, here's a set of intermediaries who have contractually committed to do nothing more than active routing in my language. And, if so, they're bound by this set of policies, which is pretty simple and easy to understand.

But then everybody else falls into whatever we call it, value added, payload touching category, in which case you've got the whole DURSA unraveling in front of you. If that sort of dichotomous line is true, it would mean that NHIN Direct, in effect, is the passive routing by definition, I'm sorry, in the active routing bucket. And, if it's not, if an NHIN Direct user application goes into the third bucket, it's got to step up to the full battery of policies.

Paul Egerman – eScription – CEO

This sounds very useful, David. Could you just go back and describe active routing again versus value added?

David Lansky – Pacific Business Group on Health – President & CEO

Active routing means you don't look at the payload at all. You do look at the header or syntax. You maybe make changes to it if needed to improve the routing. For example, the example I gave yesterday of the lab data where the NPI is wrong. It has to be tweaked, or the NPI is moving and it has to be tweaked.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

David, this is Micky. Could we just define the key term here "header" because I take header to mean the addressing information, which you would need for what you're calling passive as well, but I would defer to Wes or Dixie if I'm getting that technical definition wrong.

David Lansky – Pacific Business Group on Health – President & CEO

I agree with you, Micky. I only meant that in the active terminology, you also make changes to the header to improve the addressing....

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

I'd like to suggest that we come up with our own definition that is understandable to the committee members.

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

I agree. There are headers in the headers.

Paul Egerman – eScription – CEO

Yes, and so what I'm trying to understand – I'm sorry. Go ahead.

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

If my definition is too lumpy, then we'll get feedback on that, but I think that, frankly, there are two levels that we can consider, one where I'm struggling now to get out of the technical world. It's like speaking a

foreign language. One is where the protected health information about the patient is in any way other than decryption, assessable to the intermediary, and the other is where that is not true.

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

I think we're talking a postcard versus a letter in an envelope.

Paul Egerman – eScription – CEO

That's true, but hold on a second. Could we just go back quickly to what David Lansky said? I didn't quite understand the value added. Is that transforming the data, or does that go into the example that Rachel Block gave about aggregating data? What did you mean by value added, David Lansky?

David Lansky – Pacific Business Group on Health – President & CEO

I mean any manipulation of the data, aggregating, transforming, interpreting, whatever.

Deven McGraw - Center for Democracy & Technology – Director

But in the payload, right, David, not necessarily in...?

David Lansky – Pacific Business Group on Health – President & CEO

Any time the PHI is being exposed and presumably then used by somebody.

Paul Egerman – eScription – CEO

The comment I'd give is what David is trying to do is to categorize these issues, and the comments I'm hearing is we want to categorize them, but we want to do it with non-technical terminology. Does that sound like the right path for us to be on here?

David Lansky – Pacific Business Group on Health – President & CEO

Yes.

Paul Egerman – eScription – CEO

Let's walk through this. The first one he's calling passive routing, which is like the routing and below. The sense, I'm taking a guess, but tell me if I've got this wrong. Rather than wordsmith it, that is a category people – are we okay with that as a category? Okay. Then the question is, what are the other categories? The next one he described was active routing. Then he does value added. Does somebody else have a way to do this that's non-technical?

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

This is Wes. I'm proposing that as a working assumption that we need only two categories rather than the three that David identified that the distinction between what I understood David to mean by active routing and value-added services is not enough of a distinction to make a difference in the policy that we might come up with. I recognize that I'm not an expert on policy, but there's a proposal on the table....

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

I think we....

Latanya Sweeney – Laboratory for International Data Privacy – Director

This is Latanya. I actually, I kind of like David Lansky's three because there are some interesting nuances that, at first glance, the idea of the active and the value added may sound different, I mean, may not sound different at one level. But I could easily imagine many situations where it could be different.

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

What would be one of those? What would be one of those? This is Wes. What would one of those be, Latanya?

Latanya Sweeney – Laboratory for International Data Privacy – Director

For example, in the active, and they could simply be the case that all I have to do is modify it, but what I have is a registry of known identifiers for the patient at different locations. In the value added, I think Rachel Block's kind of thing is a great example, and it may not be that I'm providing that service. It might be, I'm just facilitating the service by linking the people together and if they have on sight software at the final destination that does the merging.

Paul Egerman – eScription – CEO

Right....

Latanya Sweeney – Laboratory for International Data Privacy – Director

But with both of those, I'm doing routing. But in the value added routing, it's quite different than just the active routing.

Paul Egerman – eScription – CEO

Yes, but you bring up a good point, Latanya. I was struggling to make sure I understood what value added meant. Let me give a specific example. Suppose I'm doing something like what SureScripts does or Quest does where I'm translating from one version of HL-7 to another version of HL-7 or taking a transaction and putting it into HL-7, so it's the right format. What is that activity? Is that active routing, or is that value added?

Latanya Sweeney – Laboratory for International Data Privacy – Director

I would consider that value added?

Paul Egerman – eScription – CEO

Is that what you would consider it, David, David Lansky?

David Lansky – Pacific Business Group on Health – President & CEO

Yes.

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

I wouldn't consider that routing at all. That's why I have a problem with these being three categories of routing, and value added, I agree with Latanya, is a huge category that extends all the way up to the top of my pile where they're developing these integrated repositories and selling information and calling it value added.

Paul Egerman – eScription – CEO

Let me respond....

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

You know ... value added routing is.

Paul Egerman – eScription – CEO

Let me respond to the comment of routing by saying this is message handling.

Deven McGraw - Center for Democracy & Technology – Director

I'm not sure that helps.

Paul Egerman – eScription – CEO

Well, it does....

Deven McGraw - Center for Democracy & Technology – Director

...big distinction though.

Paul Egerman – eScription – CEO

It is a distinction between routing and message handling because if we call it message handling, does that solve your problem, Dixie?

David Lansky – Pacific Business Group on Health – President & CEO

Paul, this is David. Can I make one more comment about the problem I was trying to solve here?

Paul Egerman – eScription – CEO

Yes.

David Lansky – Pacific Business Group on Health – President & CEO

I'm coming at this from the business and policy side, not from the privacy and security side. What I understand is that a lot of HIEs, including the state designated ones around the country, have a business model, which depends upon what I'm calling value added functionality.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

David Lansky – Pacific Business Group on Health – President & CEO

NHIN Direct, by its sort of construction or its evolution, has been trying to stay under that radar and not include value added services in effect and stay at a lower, simpler level of or less intrusive level of data management in order to be simpler, both technically and, I think, at a policy level, and that was our charge originally was to help Arien and others. Is there a suite of policies, which is more lean and less cumbersome to engage in and less, you know, lawyerly that would expedite the adoption of that set of standards? This gradation we're trying to sort out right now to me is to both see what's underneath the radar of doing a business associate agreement, what is viable to do without triggering the ONC HIE infrastructure, and the expectation ONC has created that these will be sustainable HIEs because of their business model, which in turn almost always implicates PHI.

The business side of our discussion is, is there a set of services, which is was calling active routing, which don't trigger Bas and the ONC HIE infrastructure, and are not inherently sustainable as a business model, I don't think, although maybe NHIN and other examples Micky might have would say they are. So I'm almost coming at it from the other side of the telescope. Is there a set of functions that are serviceable without reinventing the entire DURSA, which we're going to have to spend all summery probably doing?

Paul Egerman – eScription – CEO

Here's what would help. Could you give one or two or three examples of active routing and one or two or three examples of what functions are value-added services? In other words, value added services, I think, you sort of include what I call data transformation, something....

David Lansky – Pacific Business Group on Health – President & CEO

Yes, I think ... if you have to manipulate just the header, but not open the PHI, that's what I'm calling active routing. The example I had from an HIE here is, even coming from national labs, 40% of the

messages, the header didn't have accurate information to do the transmittal, and the HIE had to open the header, fix the incorrect NPIs, provider identifiers, and fix typos in the actual ... to Wes's point, the e-mail address.

Paul Egerman – eScription – CEO

Can I just make an observation real quick?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. Paul, one quick point. This is Micky. I would just point out that that, what David just described I don't think is on this list.

Latanya Sweeney – Laboratory for International Data Privacy – Director

Right, but what I was....

David Lansky – Pacific Business Group on Health – President & CEO

That was syntax changing, Micky.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

No, syntax is checking the structure of the payload.

David Lansky – Pacific Business Group on Health – President & CEO

Okay.

Paul Egerman – eScription – CEO

Yes, it's also, the issue is, you can't really open part of the message, right? I mean, if you're able to open up what you call the header or the metadata, you've got to decrypt the entire message. You may not touch what people are calling the message contact, but you can't just decrypt part of it. You've got to somehow – it's sort of like if you open a Word document and you just want to fix the title of the document. You can't fix the title of the document without opening the whole document.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. I think Dixie's point was the data elements could be themselves encrypted. Correct?

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

Exactly, that you had a blob of data that's encrypted in there.

Latanya Sweeney – Laboratory for International Data Privacy – Director

This is Latanya. I just wanted to clarify the distinction because Wes asked me for an example, and since David's example didn't quite satisfy, I think, the kind of thing Wes was asking from me. I just wanted to clarify. There is a model out there, for example, a commercial model, where they provide security features as an intermediary by actually already sort of knowing what the identifiers are for the patient at different locations. And so when the local provider makes a request using only his own identifier for the patient, they could do what Rachel Block identified because they actually know what the identifier is for the patient at other locations and can actually take the one request and produce additional requests of the others and provide a consolidated and have them all forward back to the original recipient without reading the payload, just only looking at the....

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

Yes. If I could....

Paul Egerman – eScription – CEO

Let's make sure we ground this discussion. Let's make sure we keep in mind what we're trying to do. We're trying to categorize the kinds of messages and the kinds of activities that go along by these intermediaries so that we can use those categories to determine policies.

Deven McGraw - Center for Democracy & Technology – Director

We are, but, Paul, this is Deven. I actually think that we're starting to engage this conversation at a much greater level than might be necessary to put whatever policies we think are important for NHIN Direct, and I acknowledge that what this conversation is reviewing, if nothing else, is that NHIN Direct is such a tiny, small slice, and is cabined with parameters that have already been set by the technologist. So in some respects, it's a little bit of a false set, not a false, but an odd set of choices that we're making because we're addressing a finite universe that's already sort of been somewhat predefined. But having said that, we could spend the rest of this call going really deep into this conversation, one that we need to have, but it's also engaging issues that get to sort of greater levels of intermediary access to data that I'm not sure makes sense to do, given the schedule that we set for ourselves.

Paul Egerman – eScription – CEO

What are you suggesting we do, Deven?

Deven McGraw - Center for Democracy & Technology – Director

My suggestion is actually that rather than trying to tackle Dixie's spectrum of risk because it does talk about, and we will have to deal with it. I'm just talking about whether we do it now on this call or later in later meetings when we're trying to grapple with this in a more fulsome way that we sort of limit ourselves to the message handling policies that are necessary for NHIN Direct, as NHIN Direct has been presented to us, since that's what we've been asked.

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

That's what we have been doing.

Paul Egerman – eScription – CEO

Yes, as the NHIN Direct is presented to us, NHIN Direct does deal with all these issues.

Deven McGraw - Center for Democracy & Technology – Director

No, except it's been presented to us in ways. There's minimal functionality of the intermediary, right?

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

No, that's not...

Paul Egerman – eScription – CEO

No, not at all.

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

No.

Paul Egerman – eScription – CEO

It's presented where the intermediary can do these value-added services.

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

Exactly.

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

I'm sorry. How is that presented?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

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

Where--?

Deven McGraw - Center for Democracy & Technology – Director

Where is that?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes, so I....

Paul Eggerman – eScription – CEO

...that's in the spreadsheet.

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

...four implementations do value added. Two of the NHIN Direct implementations do value added.

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

NHIN....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. I was going to suggest that at least from what's been implied, and the reason we have this tiger team is because it hasn't been explicit, right? I think we're all just trying to sort of say what NHIN Direct is from a policy perspective, but part of it is that it's fluid. But it seems to me that from a lay perspective at least, and just gleaning, being a part of the working group, the things that seem to be within the scope of what NHIN Direct is talking about, if I just look at this list, seems to be the routing only.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Perhaps the syntax checking, no change, and perhaps the payload exposed, not modified, right? Wes and Dixie, you're close to that.

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

I don't agree with that.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Is that right?

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

No.

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

The NHIN Direct, the only thing that the NHIN Direct people have a consensus on is a list of requirements. I know that some of the people are saying for the advantage of our approach is that it does

this stuff too. I'm not aware that that is a reasonable way to characterize what the NHIN Direct group, as a consensus, thinks it's pursuing.

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

I think if we're discussing NHIN Direct, this is Dixie Baker, we should at least think about the four implementations or at least three of the four anyway that are compliant, and one does take the payload. The HIE implementation does take the payload, and it manipulates it, and it applies metadata, and it converts it into a CDA compliant document.

The second one that is the REST implementation, which is the one that we actually recommended, does take the message and does the whole F MIME thing. It encrypts it, and it digitally signs it, so it does expose the PHI. So I would say that both of those are what David has categorized as value added.

David Lansky – Pacific Business Group on Health – President & CEO

Yes.

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

I would like to suggest that we need to take those conclusions about NHIN Direct and get them validated because my understanding is a bit different, which is that the restful implementation assumes that that encryption is done at the endpoint rather than by....

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

Well, I'll send you the picture.

Joy Pritts – ONC – Chief Privacy Officer

Can we take the discussion up a level and instead of – I'm a little concerned that if we get too far into the details of these four proposals that we won't get to the kind of general policy, to address the general policy, and that we'll get into the weeds really quickly here.

Paul Egerman – eScription – CEO

I agree.

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

I think we have to establish a level of detail, and Dixie is making the point that this is the appropriate, this is the important level for providing information back to NHIN Direct.

Paul Egerman – eScription – CEO

Yes. What I'd like to hear is from Micky and Rachel. Is this the right way to categorize it because it seems like they know the real world of how to.... Is that an appropriate question to be asking?

Deven McGraw - Center for Democracy & Technology – Director

It depends on your scope of real world. There's a big real world out there.

Paul Egerman – eScription – CEO

I know, but I'm talking about as it relates to....

Deven McGraw - Center for Democracy & Technology – Director

Right, of which what we're trying to – you know, when there's intermediary access to data that's in a broad range, as is illustrated very well in our discussion and in Dixie's document, if we're trying to slice of piece of that versus taking on that whole universe.

Paul Egerman – eScription – CEO

Yes, but it's part of slicing the pizza. Maybe Joy has to correct me. I thought we were trying to provide guidance for ONC because they're sort of under the gun. They funded these HIOs, HIEs, and they have questions being asked of them ... provide value would be....

Deven McGraw - Center for Democracy & Technology – Director

I'm not suggesting that it's permanently off the table, but I guess I would ask you what your conception is of what the HIO discussion was in July because that's what I thought we were – in other words, I thought the way we sliced it was simple, directed exchange. What are the policies that need to be in place for that piece of it? And we have conceptualized that as NHIN Direct, whether that's the right conceptualization or not, I don't know. Then moving on to more robust models, not to say that it's permanently off the table, but if we're trying to think about how those policies apply to this slice based on that functionality.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Deven, this is Micky.

Deven McGraw - Center for Democracy & Technology – Director

Let me let Paul go, please.

Paul Egerman – eScription – CEO

Here's the basic problem, basic challenge that we're wrestling with is what you're saying is NHIN Direct relates to this other thing that we call directed exchange. You're making like that's one-to-one. I think that's what you're saying, and I think that's what David Lansky is saying. However, that's not what these spreadsheets are saying that's coming out of Arien. What he's calling NHIN Direct goes far beyond directed exchange. It includes all this intermediary stuff. That's why he's putting forward these questions.

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

We have a spreadsheet from Arien, directly from Arien?

Deven McGraw - Center for Democracy & Technology – Director

No, that's a standards committee spreadsheet.

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

Okay, so we don't have that directly from Arien.

Paul Egerman – eScription – CEO

No, we have two questions from Arien. This is one of them though.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Arien has asked the exposure level question.

Paul Egerman – eScription – CEO

And he gave the examples of SureScripts and Quest are the laboratory of transforming data when he asked the first question.

Latanya Sweeney – Laboratory for International Data Privacy – Director

If that's what he's asked, can we work on that one?

Paul Egerman – eScription – CEO

That's what I'm trying to do, which is, in some sense, I'm saying the split boundaries aren't the question. It's about message handling. In other words, that's why I'm saying it's about the intermediary. It's about message handling. The question is, when some intermediary handles a message, what are the policy boundaries that you're going put on it for various levels of PHI exposure? It's why I thought that David Lansky's categorization was helpful. It's also why I thought Dixie's description was helpful too. Dixie had, perhaps, a little bit too much detail.

I'd like to categorize it and say, well, passive where there's no PHI exposure, that's one thing. There's the number three, the value-add where it's data transformation. That's another category. And there's something in the middle, which I have to say I don't quite understand where you look at it and you make little changes. If we could come to agreement with those categories, then we could talk about what would be the policy implications for each of those categories.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Paul, this is Micky. I wonder if we can draw these lines into buckets that have sort of the first one is the first three, the no intermediary, just sort of cording those off and say we're not dealing with those here, correct, because there's no intermediary?

Paul Egerman – eScription – CEO

Well....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Well, let's just put those in a bucket. So there's no intermediary, that's one bucket. And then second, I wonder if then we have a grouping that basically says one category is that you are only routing, so you're providing the U.S. Post Office service, which is, you just look at the address, and you send it. You do not change anything, even in the address, and you certainly don't open the message.

Paul Egerman – eScription – CEO

Okay.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Then a second category is where you actually open the message, but you don't change anything, so that would be the syntax checking with no change, or even the payload exposed, not modified, because you've opened the message, but you haven't changed anything. Then the third category would be the category where you actually do change, and that could be the routing only, which the one that David talked about where you change the address. The second category would be that the open the message, and you actually change something, whether it's syntax, or you even go into the death spiral of actually modifying data itself, the payload.

Paul Egerman – eScription – CEO

Okay, so....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

...those are helpful.

Paul Egerman – eScription – CEO

That's actually extremely helpful, although I wrote that down. I took what you said, Micky. I wrote it down. It's four buckets, so four categories. The first one is no intermediary, so that's a category. The second is an intermediary, intermediary that only routes the data, but doesn't access it in any way. The

third one is an intermediary that, through its process, needs to access it, but doesn't change it. And the fourth one is it accesses it, and it changes the message. What do people think about those four categories?

M

Say that again.

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

Yes.

Paul Egerman – eScription – CEO

Let's go through it again. The first category, this is really Micky's I'm repeating here. The first category is no intermediary, so things go from point A to point B. The second category is an intermediary that routes or retransmits data, but doesn't access it in any way. It doesn't open the message. The third category is somebody that opens the message for one reason or another, but does not change it in any way. And the fourth one is somebody that opens and changes it before it transmits it.

M

Paul, just one refinement: In the fourth, I would have also put, they didn't open the message, but they changed the address, which is what David was talking about with 40% of lab addressing is wrong, but they changed something.

Deven McGraw - Center for Democracy & Technology – Director

How do they know what's wrong if they don't open it?

M

Because the routing doesn't work. The person's name is wrong or whatever.

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

So it's really change.

Paul Egerman – eScription – CEO

So the fourth one ... they alter the message or some transformation that occurs.

M

Exactly. Right.

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

And if you want to carry it all the way to the top, then the fifth one would be retained.

Paul Egerman – eScription – CEO

Yes. And so....

Gayle Harrell – Florida – Former State Legislator

It's Gayle. Where would you put messages that are aggregated?

Paul Egerman – eScription – CEO

We put that in the retain....

Deven McGraw - Center for Democracy & Technology – Director

The retain bucket.

Paul Egerman – eScription – CEO

Yes. In other words, we're sort of also drawing a line there. This is actually, I just sort of drew the line a little bit differently than what Deven did earlier. We can get to the retain bucket, the example Rachel gave of aggregating messages. That's our discussion for next month.

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

So we're saying the policy is NHIN Direct cannot retain data by definition.

Paul Egerman – eScription – CEO

I'm not necessarily saying that. I'm just saying we haven't talked about it yet when it comes to retaining the data. I'm just saying, this just message handling. This is just....

Carl Dvorak – Epic Systems – EVP

Paul, this is Carl. Should you put on the one through four categories the stipulation that it's not retained?

Paul Egerman – eScription – CEO

That would be good. The only question there is going to be is what about audit trails. Do we say not retained, except audit trails?

Carl Dvorak – Epic Systems – EVP

I'm wondering if it needs to be retained for audit trail purposes. I'm not sure that it does.

Paul Egerman – eScription – CEO

Category probably does. If you're going to transform the data, you ought to keep an audit trail.

Carl Dvorak – Epic Systems – EVP

That one possibly, I agree with that. I meant for the first two for sure, and possibly the third one.

Josh Lemieux – Markle Foundation – Director Personal Health Technology

Paul, this is Josh Lemieux. I'm just wondering. There's got to be some audits of message went from point A to point B. Doesn't there have to be?

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

Yes.

Josh Lemieux – Markle Foundation – Director Personal Health Technology

Don't you retain...?

M

Right ... audit, audit trail.

Paul Egerman – eScription – CEO

That's a great question, but you know what's going to be easier for us to do is define retaining data. Retaining data would be retaining data in a way that's accessible by patients and then perhaps is intended to be accessed by somebody.

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

Retaining patients. Retaining patient data, so other than audit trails.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. Is it retaining payload?

M

Yes, I was going to say you could audit without retaining the message, and I think....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right.

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

Yes, retaining.

M

Most places that do in the one to three category don't actually keep the messages because then you have to worry about the key becoming later compromised or certificate becoming compromised.

Paul Egerman – eScription – CEO

I sort of screwed up this discussion by raising the audit trail issue because I'm showing that tripped us into another discussion because the main concept though was retaining PHI, which is getting back to something that Gayle had said and also Rachel had said that the main thing is retaining PHI, aggregating PHI, that's yet another category. That's not what we're talking about in these four categories. This is simply a message.

A message can be anything. It can be an order, a result. It can be an entire CCD or CCR, but it's a single message going from one place to another, possibly through an intermediary. And so my question is, do we have four categories here that are comfortable then to frame our policy discussions about what would be the policy boundaries for each of these four. Again, four boundaries: The first one is no intermediary; the second one, routing, but no access; the third is intermediary looks at the message, doesn't change it; and the fourth one is some transformation occurs.

Deven McGraw - Center for Democracy & Technology – Director

That sounds good.

Paul Egerman – eScription – CEO

Can we roll up our sleeves now and talk about each of these four? Is that the right way to approach this, Deven? In other words, if I'm looking at this right, if we're talking about each one of these four, and we get through all four, then we've answered the question.

Deven McGraw - Center for Democracy & Technology – Director

Right. Yes. It's almost as though one and two, which is either no intermediary or routing only and no access – never mind. I lost my train of thought, but they sort of seem quite similar in terms of exposure. The question that we started with, which is, how much PHI is exposed, they sort of seem very similar to me.

Paul Egerman – eScription – CEO

What do we want to say then from a policy standpoint? Do we want to put a gold star next to them and say way to go, and...?

Deven McGraw - Center for Democracy & Technology – Director

Yes. I mean, it almost gets to the point of okay, so what do we mean? And maybe we want to put some parameters around what we mean by exposure, which was this point that Micky raised in an earlier call, but it could be phrased as if there is no exposure by our definition, it's either no intermediary is used or it's routing only. Then that certainly is, and we wouldn't have to put any additional requirements on it that would flow from entities that do have access to it, like you can't reuse it, or you have some limits on how long you can retain it, etc.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. Do we want to have some policy about what can and cannot be included in the header for addressing purposes?

Deven McGraw - Center for Democracy & Technology – Director

That seems very specific from a policy standpoint, but tell me what you're thinking there. I see that sounds almost more like a best practice to me, so you have sort of an overarching principle of sort of limited data exposure for message handling, you know, limited to the purpose necessary. And in models one and two, given those functionalities, there isn't a need to. But in terms of what are you thinking in terms of specifically what needs to be in the header, because that seems to be very directed to different....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I guess what I was thinking is, just to take a craft, and this is probably maybe a stupid example. What if an organization decided I'd love to be able to include in the header that this is an abnormal result so that it can be processed on the other end just from the header that this is an abnormal result, and are we okay with that?

Deven McGraw - Center for Democracy & Technology – Director

But in terms of my question, that seems to be in model three if the intermediary – in other words, they can see that message, even if they're not opening it, right? Or is there something I'm missing here? If you're just routing it, and there's no access—

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

No, but I'm saying, this would be in the address itself that someone decides that in the addressing information that that's all that that router who doesn't open up the message, it's on the outside of the envelope. So this would be U.S. Post Office, I put down I want to send a letter to Deven McGraw (your lab result is abnormal). I decide to put that on the envelope because it's helpful to you because then you don't have to open up the letter.

Deven McGraw - Center for Democracy & Technology – Director

Then that messes up my conception of the four models then because I was not thinking of a routing only, no access model as having that level of identifiability across the envelope.

Paul Egerman – eScription – CEO

Right, because then....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Well, but that's a good question. What do you put up there?

Paul Egerman – eScription – CEO

Let me make a suggestion, Micky. You're raising a great question because routing only should mean, well, gee, I'm like the letter carrier. I get something, and it says this goes into post office box 23. I take it,

and I put it into 23. But you're saying, well, maybe there's something more you're going put there, which is, this is special delivery. This is a priority. You've got to put this ahead of everything else.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right, exactly.

Paul Egerman – eScription – CEO

...23, and so what you could say though is now we're going to put a little bit of a definition or boundaries about what is allowed in this routing only thing because, again, it's sort of like the special delivery example. That probably is okay, but maybe there's something else that's not okay.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right.

Paul Egerman – eScription – CEO

What I'd like to do is try to see if we can get some momentum and tackle the other two, so why don't we ask you? I don't know if Rachel or anybody was able to help you to write us a little proposal as to what you think would constitute acceptable, additional delivery instructions, as it were, to still be making it into a routing only.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Sure. I'm happy to take a stab at that.

Paul Egerman – eScription – CEO

Okay, so then why don't you do that, and you could do that as like an e-mail or something. Is that acceptable to everybody?

Gayle Harrell – Florida – Former State Legislator

Yes.

Deven McGraw - Center for Democracy & Technology – Director

I think it's fine, although I'm trying to think if we have to wait for that in order to make some progress on some....

Paul Egerman – eScription – CEO

No, I don't think we have to wait for that.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Paul Egerman – eScription – CEO

I don't think we have to wait because I think what we're saying is for no intermediary for routing only, we understand those things, and we also understand the policy implications. The policy implications is good job, gold star, we don't have to say anything. Is that right?

Josh Lemieux – Markle Foundation – Director Personal Health Technology

This is Josh. It seems like we do want to say something. If that's what they say that they're doing, then clearly that's what they have to do. They're not retaining and they're not accessing the information.

Gayle Harrell – Florida – Former State Legislator

They still have to deal with the audit trail of what is sent where, and what safeguards are you going to put around access to those audit trails?

Paul Egerman – eScription – CEO

You're raising a good question, and that was Gayle.

Gayle Harrell – Florida – Former State Legislator

Yes.

Paul Egerman – eScription – CEO

And so I say that also asking people to say their names, but excellent observation. So are we saying for the one that's routing only that our rule is no audit trail?

Deven McGraw - Center for Democracy & Technology – Director

No, no. What?

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

We have another question, right? We have a question that is tied to the original question about audit trails that we need to come up with....

Deven McGraw - Center for Democracy & Technology – Director

Wait a minute. Why did we get on audit trails in the first place? Let's lift this discussion up a little bit to the core question of, in other words, this feels like it's going off track a little bit. The core question – I think where it sounds like we're headed to me is where there is no to very limited access to information about a patient, certainly there are some core policies that we would put in place, but not necessarily higher level policies that govern their use of that data and limit it and limit the reuse, right? In other words, you get a gold star if you choose these less, I'm just going to call them less intrusive models as shorthand, then the number of policies that you need to adopt, and you're going to be held responsible to, is consistent with that very low or no level access to data versus at a higher level of access to data. We've got a whole host of other things we're going to require of you and hold you accountable for.

Paul Egerman – eScription – CEO

Also, instead of using the expression gold star, maybe we should say, well, this is a best practice.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

We're saying this is the best practice. Now what Gayle asked is what happens if they keep an audit trail?

Deven McGraw - Center for Democracy & Technology – Director

Right, but can we...?

Paul Egerman – eScription – CEO

And my question is ... doing routing only? I don't think you do keep an audit trail.

Gayle Harrell – Florida – Former State Legislator

Does it happen? I don't know.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. I think a couple of thoughts. I think, Deven, one thing here. I understand the line that you're trying to draw or the distinction. I think that the issue though that a number of us are raising is that there is discretion in what people can put into an address, and so we may just need to deal with that issue.

Paul Egerman – eScription – CEO

Right, but I'm saying let's keep that as a side discussion.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes. Exactly. I agree with that, so we can move forward. The reason that that's important for the audit trail discussion, and the reason audit trails are important is just from a service level perspective. If I am a routing agent, and that's all I do is routing, I may still want to keep an audit trail because if there's a message failure, I want to be able to tell my customers, it was sent, and here's where the failure was.

Now that audit trail doesn't have to keep the whole message, as I think Carl or someone was mentioning. Indeed, in most cases, I think it wouldn't for a simple routing function, but you would want to keep. It was sent from this person. It was sent to this person, and here was the addressing information I had.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Gayle Harrell – Florida – Former State Legislator

In malpractice cases dealing with lab tests.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right, because you would want to keep that, right, to protect yourself. But I agree. I think that's in the category of what we were talking about of this side exercise that I'm happy to provide something on, which is how do we set some parameters around what can be in the address. But I agree with Paul. That shouldn't sidetrack us here.

Paul Egerman – eScription – CEO

Where do we stand on the discussion? Are we ready to move on to the next category, which will be exciting? I say exciting because we open the message. Are people ready to move on, or is there something more we should talk about in these two categories besides saying best practices?

Gayle Harrell – Florida – Former State Legislator

One more thing I want to add to that thought, it's Gayle, is the authentication of the recipient.

Paul Egerman – eScription – CEO

We're going to get to that.

Deven McGraw - Center for Democracy & Technology – Director

...get to that.

Paul Egerman – eScription – CEO

Gayle, we're going to get to that as our next question. This is just, we did this a little bit out of order, but this is just handling the message. We will talk about authentication and credentialing is the next question. It's a very interesting question.

Gayle Harrell – Florida – Former State Legislator

Okay.

Paul Egerman – eScription – CEO

Deven took the no intermediary and routing only and put them together into one category.

Deven McGraw - Center for Democracy & Technology – Director

Right, with the TBD on whether we want to place some limits on what would be in a header.

Paul Egerman – eScription – CEO

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Or maybe say that if you have all this information like patient status or type of message that you might actually get bumped to a different category, a higher level.

Paul Egerman – eScription – CEO

That's right. We're going to put some definition about routing only.

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

I disagree with lumping those together—this is Dixie Baker—because one is no intermediary, and one is. So there's policy that we will need to define for that intermediary in the one case, and in the other, it's like we don't care.

Paul Egerman – eScription – CEO

But what is the policy...?

Deven McGraw - Center for Democracy & Technology – Director

No, but I think we always care, Dixie. I don't disagree with you that there's a distinction between the two. This is Deven. But in terms of data exposure, if they're routing only and not accessing it, I'm having a hard time figuring out what the distinction is on that particular point.

Paul Egerman – eScription – CEO

Or to put the question differently, Dixie and Deven, for this one that's routing it only, we want to just answer this question. What other policy statements do we want to make other than say it's a best practice? Is there anything else that we have to say?

Deven McGraw - Center for Democracy & Technology – Director

We're simultaneously trying to build the whole framework about data security.

Paul Egerman – eScription – CEO

That's it. There'll be those things. There'll be some security issues.

Deven McGraw - Center for Democracy & Technology – Director

In terms of sort of....

Paul Egerman – eScription – CEO

In terms of BAA or consent or anything, that stuff doesn't – in other words....

Deven McGraw - Center for Democracy & Technology – Director

But for a particular set of policies with respect to the data within, the information within, that seems to me that that's obviously of less concern here.

Paul Egerman – eScription – CEO

Okay, so....

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

I thought we need policy to even define what a passive intermediary can do. And if there is no intermediary, we clearly don't need policy. But if there's an intermediary, I think we need to define here is, you know, if you claim to be a passive message handler, here's the policy of what you can do....

Paul Egerman – eScription – CEO

Let me ask you a question, Deven. Can you live with making these two separate categories?

Deven McGraw - Center for Democracy & Technology – Director

Yes. No, of course. They are two separate categories.

Paul Egerman – eScription – CEO

We'll keep them as two separate categories, Dixie. We're saying both are best practices. I guess no intermediary is really probably the best ... best practice.

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

Yes.

Paul Egerman – eScription – CEO

Are we ready to move on to the next category, which is opening the message without altering it?

Deven McGraw - Center for Democracy & Technology – Director

Yes, go ahead.

Paul Egerman – eScription – CEO

Category number three, we're going to open the message, and we're not going to change it. That's what the intermediary is going to do, so what do we want to say about that from a standpoint of policy boundaries or comments?

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

I think we have to define this. Maybe this is where we define the one of, can they, you know, like what the REST implementation does? Does this include that they can encrypt it and apply a digital signature? Are those things that they can do to that open...?

Paul Egerman – eScription – CEO

Again, the difference between category three and four is category three, as Micky laid it out, was somebody opens the message for whatever reason, but doesn't alter it.

Deven McGraw - Center for Democracy & Technology – Director

Right.

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

That's what I'm saying. Does encrypting it, is that part of altering it?

Paul Egerman – eScription – CEO

I would go out on a limb and say no.

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

Okay, then we....

Paul Egerman – eScription – CEO

Altering it means you're doing something different to whatever the message says. Did I do that right, Micky?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes, I would agree with that.

Paul Egerman – eScription – CEO

I think, encrypting it, I would not count as altering it. In fact, that could be an example of number three where somebody sends you a message, and they don't have the level of security that they really should have when they send it to you, so they encrypt it, but you are on the second level of security ... Dixie, so maybe they encrypt it, and the intermediary then adds the SMIME, reencrypt it, and shoots it to wherever else it's supposed to go, but that hasn't changed the message that's improved the security.

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

What I'm saying is....

Latanya Sweeney – Laboratory for International Data Privacy – Director

...but I would add though, but if they encrypt part of it, they are changing it. It's one thing if they take the whole message as a unit and encrypt it, but if they encrypt only part of it, they are changing it.

Paul Egerman – eScription – CEO

You lost me there. Is that right? Is that Latanya who just said that?

Latanya Sweeney – Laboratory for International Data Privacy – Director

Yes.

Paul Egerman – eScription – CEO

Okay. You say that, I'm surprised. It must be correct, though, if you said it. I don't understand that at all, but that's okay.

Latanya Sweeney – Laboratory for International Data Privacy – Director

What we do often is we don't look at privacy in a vacuum, but across utility and other constraints. And so they increase the provider's liability if part of the data is encrypted, and the provider ends up getting it and can't see that part.

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

That's a good point.

Deven McGraw - Center for Democracy & Technology – Director

Right, but what would be the point of encrypting it to the level where the provider who was supposed to see it couldn't open it?

Latanya Sweeney – Laboratory for International Data Privacy – Director

Well, because it might be that you're encrypting part of it saying that the intermediary is making a judgment decision that that provider doesn't get to see this part of the message.

Paul Egerman – eScription – CEO

Let's look at this category also in the context of looking at the final category. In the final category, they're talking about transforming the message, right? To me, transforming the message is more the example of what happens all the time where it goes from 3.3.6 to 3.7 version of HL-7. Somebody takes two fields and makes one field a little bit bigger, puts in some lead zeros, moves field place one to field place two. They do something that's actually fairly mechanical, but they still rearrange the furniture, then the message continues on, but that's the intention of the final category.

My understanding of this category was that that was not occurring.

Latanya Sweeney – Laboratory for International Data Privacy – Director

Right, and I'm just saying that I agree with what you and Micky said that if they encrypt the entire message it's really no change. But I was just saying that if they encrypted part of it, I would stick it in the fourth category.

Paul Egerman – eScription – CEO

That's a comment that's like the comment about Micky's about the headers, which is, we're going to do perhaps a separate discussion where we try to draw sharp lines around these categories. I'd like return to this category of opening a message and not changing it, which I think the example Micky gave was, you check it to make sure the syntax is correct. It could also, suppose, be just the way the intermediary works. It lands on their site. They open it. I guess this is the issue. If they open it, then they reencrypt it, does that mean that that's a change?

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

This is Wes. Are you asking the question, A, is this ever done, that an intermediary reformat the content of the message without changing its intent, or are you asking a different question?

Paul Egerman – eScription – CEO

I'm asking the question, when this occurs, what should be the policy boundaries? In other words, when this occurs, are we going to say that's a best practice? Are we going to say you need to have a BAA or some other contractual approval? Are we going to say this is a patient consent issue? Is this a disclosure issue? Is this a big deal? Is this a little deal? How do we do we view that thing?

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

I'd like to suggest that you have access to the data, that the context ... of syntax checking of the syntax of a message with encrypted data provides very limited functionality for checking the syntax, and I've actually never heard of being used ... not an example because ... because they don't have an intermediary. But it provides access to the data, so it's a BAA level of policy....

Paul Egerman – eScription – CEO

That requires – we're saying this occurs. You're suggesting that if this occurs, that puts it into like the BAA category of policy issues. You should have a business associate agreement. You should have some contractual protection, and that organization should represent an organization that you have some level of confidence in.

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

Yes. Paul, you use that term as, I thought, a good sort of broad categorization of how big a deal is it. While I can't say I'm an expert on all of the requirements for business associate agreements, I think it's a pretty big deal because they can see the data. And, therefore, I have to be able to spec them to do all of the things that I would have my own employees do with regards to stewardship of that data.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

Okay.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I'm sort of trying to think about this in a sort of broad policy concept. As a result, I'm actually struggling a bit to see. I mean, I understand the functionality distinction between model three and four, but from a policy standpoint, if you have access to identifiable data, and that includes whether you change it or not, you ought to be held accountable for what you do with that data. And the business associate agreement is a mechanism for doing that. I think we need to say the parameters that need to be addressed in business associate agreements, such as limitations on sale or reuse, data retention, the sort of cadre of data stewardship policies that Wes referred to. That really attaches any time you've got access to this data, regardless of what you do.

Gayle Harrell – Florida – Former State Legislator

I could not agree with you more, Deven. I think it's absolutely essential if you have any access you can view, if you have any access whatsoever. You need to have a very high level of responsibility and security around that.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

If I heard you right, Gayle, and I heard what Deven just said, both of you are saying, well, whether or not you transform the data doesn't matter. You're saying the policy implications of accessing it are the same as the policy implications of changing it.

Deven McGraw - Center for Democracy & Technology – Director

Well, sort of. Actually, Paul, this is Deven. When you put it in that context, there's likely at least one additional piece that's implicated when the data is changed, and that is, if you are putting out there as an intermediary that you are going to change data in a way, for example, to make it into the structured content that it's supposed to be, you have to essentially stand by your ability to do that, right? You're putting out there that you can change data into the right structure. You ought to be held accountable for doing that.

Paul Egerman – eScription – CEO

That's right, but that's....

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

Yes, and liability. You should take on liability because it affects patient safety.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

The question though is, is that just a contractual representation? Is it a liability issue? Or is it a privacy and security issue?

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

This is Dixie Baker. I suggest we put the cutoff on NHIN Direct below changing something. NHIN Direct should do more than open the message with no change.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

This is Micky. Do we want to say what NHIN Direct should do, or are we saying here are these buckets. We're talking about policies for each of the buckets, and wherever NHIN Direct falls, it falls, but then ... policy implications depending on what it says it's going to do.

Paul Egerman – eScription – CEO

I kind of agree with you, Micky. I think that's what we need to be doing. In other words, we're not trying to direct Arien's group necessarily as much as use the real world's input as to what he's dealing with to help us understand these issues.

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

I think there's a huge leap in risk between looking at the message and changing anything. Once you start changing the address, once you start changing the content, the lab value, there's a huge leap in risk.

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

I think we all agree with that, right?

Deven McGraw - Center for Democracy & Technology – Director

Yes. I don't think anybody disagrees with that.

Paul Egerman – eScription – CEO

So in some sense, we're saying the policies for the last two are the same, except if you transform the data, you have additional. You're making an additional representation. You're transforming it correctly, so you're talking on a responsibility, an additional responsibility that needs to be reflected somehow, I suppose, contractually. Is that a fair summary of that?

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

The last two, what do you mean? The last two are the same.

Paul Egerman – eScription – CEO

The last two categories, but....

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

No, they're not the same. No, they're very, very different.

Deven McGraw - Center for Democracy & Technology – Director

No. Dixie, this is Deven. I think what Paul is saying is we would want to set on the last two a very similar set of policies with respect to reuse and retention. I mean, we want to have policies that address reuse and retention of data for any model that involves actually accessing data. Then there are additional considerations that come to play that need to be addressed, whether they're privacy and security or a

liability. What bucket you put them into doesn't matter, but they need to address that this kind of alteration or transformation of data is properly done.

Paul Egerman – eScription – CEO

Let me see if I can hear what you just said, Deven, and ask if that's an adequate answer to this question. For this category where the message is opened, but not changed.

Deven McGraw - Center for Democracy & Technology – Director

Can I interrupt you and just ask somebody who is in a room where another conversation is going on to please mute. Thank you.

Paul Egerman – eScription – CEO

For this category where the data is accessible, but not changed, what you're saying is the policy boundary, the policy implication is that a BAA is required and that, in addition to the normal sorts of privacy protection, it has to also address issues relating to data reuse and data retention.

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

I see. Yes. I agree. I agree.

Paul Egerman – eScription – CEO

Now is that an adequate response, Deven, in terms of – in other words, I'd like to be able to go to Joy and say we answered the question. Is that an answer to the question for this category?

Deven McGraw - Center for Democracy & Technology – Director

Yes, I think it's the – whether we want to say more specifically what we would do for reuse and retention, that's another issue, but that certainly is, I think, a very good start.

Paul Egerman – eScription – CEO

Then for the final category, the fourth category where there's some transformation occurring, what we're going to do is we're going to say—

Judy Faulkner – Epic Systems – Founder

I'm going to have to call Lenard, that guy up....

Deven McGraw - Center for Democracy & Technology – Director

Carl, can you either mute, or if Judy has a comment to make, if she can be louder about it?

Paul Egerman – eScription – CEO

For the fourth category, I think, if I'm hearing the discussion ... a business associate agreement is required that does everything we just said for the prior one. It deals with reuse and retention. And, in addition, there needs to be some representation, contractual representation about the accuracy and quality of the transformation.

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

And liability.

Paul Egerman – eScription – CEO

That's right. In other words, the idea is the representation creates the liability. Sure, and liability.

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

Yes.

Paul Egerman – eScription – CEO

To go back to the original question is, what were the policy boundaries for varying levels of PHI disclosure and message handling. Did we answer it?

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

Yes, but we should make it clear that we believe that it's not just a matter of PHI exposure. It's also a matter of patient safety because we've also addressed that.

Paul Egerman – eScription – CEO

I'm not sure we necessarily....

Deven McGraw - Center for Democracy & Technology – Director

We haven't completely addressed it. We certainly touched on that issue.

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

Yes. We've touched, yes.

Paul Egerman – eScription – CEO

Probably perhaps more precise to say it's not just the level of PHI exposure. It's sort of like what's the actual activity that's going on.

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

Yes. I agree.

Paul Egerman – eScription – CEO

Do you want me? Part of me wants to review this. Part of me is afraid to review it because I'll open the discussion again. Correct me if I'm wrong, Deven. I think we should declare victory. We answered the first question.

Deven McGraw - Center for Democracy & Technology – Director

I think we should too, and we can promise the group our articulation of it for final review.

Paul Egerman – eScription – CEO

Let me say thank you to everybody. We answered the first question. We're actually making terrific progress. This is hard stuff.

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

Yes, it's hard stuff.

Paul Egerman – eScription – CEO

This is hard stuff because – and so I want to thank everybody for sticking through this one before we do the next one, which is harder. But this is hard stuff, but this is why they're paying us the big bucks. In other words, we're trying to deal....

Joy Pritts – ONC – Chief Privacy Officer

That's right. Don't spend it all in one place, Paul.

Gayle Harrell – Florida – Former State Legislator

The check is in the mail.

Paul Egerman – eScription – CEO

...deal with....

M

You had to say that, didn't you, Paul?

Paul Egerman – eScription – CEO

Yes. I guess that was – I seem to make a really bad mistake in every call. Now that was probably a mistake in this one, although maybe there's still a chance for me to really screw up, continuing on. But what I'm trying to say is we've got to deal with the difficult issues, so I appreciate everybody hanging in there, as we go through this. I guess what I'm going to say is we should take a deep breath and open up to the second question. Are you okay with that, Deven?

Deven McGraw - Center for Democracy & Technology – Director

I am completely okay with that, Paul.

Paul Egerman – eScription – CEO

So here's the second question that was raised by Arien, which is a fascinating question, and actually got an e-mail from Neil on this. I don't think he's on the call, but it was very helpful. Here's the way Arien phrased the question. He said it was a very simple thing. It was in actually yesterday's agenda sheet that I had sent out. It said who holds the keys to the "trust level", the HIO or the provider? The question really relates, however, to the concept of centralization and decentralization of credentialing and other sort of like privacy practices.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

The fundamental issue here is if you look at the e-mail trail that Arien and I did, Arien had given an example of credit card processing. In credit card processing, it's all very centralized. There are two or three credit card companies, and they do everything. They set the rules. It's their way or the highway. And they issue the credentials. They make sure that if you're submitting a credit card transaction that you're authorized. It's very, very centralized.

The comment I gave back to Arien is that sounds great for credit cards, but that's not how it works in healthcare for a lot of reasons. One is credit cards is just money, and this is more than just money. This is people's lives. This is very serious stuff. Healthcare is inherently decentralized. This was all about decisions between patients and providers in which Arien responded back by saying yes. But, you know, doing things like credentialing and making sure you've got the right sender, that's a complicated thing. The technology that's complicated, we really want to burden the provider with that issue.

This even goes back to the question that Gayle started to ask that I sort of cut her off on is who is authorized. So the question is sort of like another way to rephrase the question that Gayle is asking. Who is supposed to determine who is authorized? Is that the provider's responsibility? Is that an intermediary's responsibility? Are we going to say each provider has got to do this straight and do this? Is this going to be centralized? Is this the HIOs? Who is going to do that thing?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

This is John Houston, and I think this all goes to something I've been talking about for a long time, which is, there has to be a central governance model, and I think it has to be very specific, and there has to be very clear accountabilities, and it can't be at a local provider level. It has to be at, I think, a national level, frankly, because you're not only dealing with this issue, but you're also dealing with issues where problems arise, where complaints arise, and you have bad actors.

Paul Egerman – eScription – CEO

Can you explain what you mean by bad actors?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Somebody does something with information that they shouldn't be. There's a patient complaint or there are issues associated with using information for one purpose when they were not supposed to, people that don't comply with whatever rules are established.

Paul Egerman – eScription – CEO

When you say bad actors, the question I'm trying to understand, John, are you referring to this is a problem that all large organizations have, or there's some employee just doesn't get the message and does something that's not appropriate, or are you talking about not within UPMC, but some bad actor being a provider or...?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

This is ... bad actor, not a person. We just put our own workforce. I'm talking about the organization that doesn't do what it's supposed to do.

Paul Egerman – eScription – CEO

Okay. So you're saying that at an organizational level. So your proposing that there should be central governance, so let's look at the issue. When he said trust level, he's referring to a lot of things. The first one was credentials. In other words, this is specifically responding to the issue Gayle raises. Who is going to decide and issue credential as to who is authorized to send and receive information? You're saying, John, it should be a centralized government function to do that?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Some organization needs to be accountable for that, like so many things that happen. It has to happen one time, but I think that then that same organization, if there is an issue about whether the organization inappropriately used information or didn't meet their obligations, whether it be because they implemented inadequate security or there was some serious breach, or somebody knowingly did something wrong. Then that same governance organization needs to go in and either discipline or remove that organization to participate in these types of exchanges.

Deven McGraw - Center for Democracy & Technology – Director

Right. This is Deven. I actually see these as two very much related, but somewhat separate questions. One is somewhat more of an infrastructure one, which is, who at least at first blush is responsible for issues of if a provider covered entity wants to exchange data with another, who is to be held accountable, especially if there's supposedly in some – there will be some intermediary in play in some of those transactions. Then closely related to that then is how do you enforce the set of policies that apply regardless of what level they apply to. I actually think they are two somewhat separate questions.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes. I agree with that. This is Micky. It seems like there are two issues we're grappling with. One is the level of granularity, which is to say that at the user level, or do we accept sort of a federated kind of model

where if Beth Israel Deaconess is a member organization, anyone we – we bend the intermediary. It's okay for the intermediary to say that anyone within the domain of Beth Israel is a responsible user by definition because we are saying that Beth Israel is a responsible user.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

But I think Beth Israel can discipline its own internal staff, if that's what you're really talking about, and be responsible for it.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

But there needs to be some roll up such that if something happens that it involves something at Beth Israel, that there's some mechanism to insure that issues are appropriately address, that there's somebody to call Beth Israel on account that something happened that was inappropriate. By the way, my other example too, I think, is meaningful here is that what happens if an organization wants to sign up and signs up for all this, but is found to have failed to implement adequate security? What's to say they're not complying with HIPAA, they're not complying with ... security, the policies we put in place? And, as a result, there are serious problems with overall safeguarding of information. How do we deal with that?

Paul Eggerman – eScription – CEO

Just a second. That's a good question, John. But I don't think that's the question that we're answering right now.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

But it all rolls up to this. Maybe I'm over-generalizing, but I roll all this up into an overall governance structure ... and an accountable party that can be the point of focus on all of these types of things.

Paul Eggerman – eScription – CEO

Your view on this is interrelated with ... Micky, sorry, go ahead, Micky.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes. What I was going to say is I wonder if – so maybe if we give a concrete example again that can help. NEHEN, and I'll find out the details, but my understanding of the way NEHEN, the New England Health Exchange Network, works is that they are a utility router at the center, but you have a set of bilateral agreements. First off, you have to apply to become a member, and there are certain criteria that you have to meet. Whatever those criteria are, we can sort of get the details if we need that to become a member. But then the exchanges are really bilateral exchanges that are facilitated by bilateral contracts between the entities.

My data would never go to another party unless I had a bilateral arrangement with them. Let's say I'm Beth Israel, and I decide that Bay State Hospital is no longer a trusted partner, I as a bilateral matter would say, I'm not going to send any more information to you. Our agreement is now null and void.

M

Yes, but how do you...?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I don't think NEHEN ever gets into that. I suppose just – sorry, last point. I suppose at some level if NEHEN finds out that, wow, ten members have decided they don't want Bay State as a part of this

anymore, then maybe they would take as a board matter, do we decide that Bay State is no longer a trusted entity at all?

Paul Egerman – eScription – CEO

Let me understand that. In that structure, again, when Arien was asking about trust level, he was really interested in credentialing. In that structure you just described from NEHEN, who does the credentialing? Who issues the certificates?

Gayle Harrell – Florida – Former State Legislator

I'd like to bring up a point that everybody is missing. I think we have the Tenth Amendment to the Constitution that says we do not want to step on state's abilities to regulate and make laws dealing with these kinds of things. At the federal level, I don't know that we have the authority to do that. Certainly within dollars that the federal government is giving you, you have some control of things. And within states that we are funding to a large degree what's happening down at the state level, but you've got to – we don't have the ability to write law, number one, at the federal level, nor does the federal government have the ability to write that kind of law when you're really dealing with state level issues.

Paul Egerman – eScription – CEO

Gayle, you're saying, in response to what John Houston said, you're saying well instead of the federal government doing it, the states should do it. Perhaps the HIEs should be responsible for deciding who is authorized.

Rachel Block – New York eHealth Collaborative – Executive Director

This is Rachel. Just a couple of observations about that: Normally I would agree with the construct that Gayle just laid out, but we're not dealing strictly here with a simple interpretation of law. For example, under NHIN Exchange, which I know we're not talking about yet, but we will get there eventually. The federal agencies who are participating in that basically either have or will adopt certain policies. And if you want to "do business with them" for the purposes of exchanging data, you must follow their policies, regardless of what your state laws might be. There is a practical level, Gayle, at which the strict interpretation of the state's ability to set forth laws doesn't necessarily take into account the complexity of other kinds of business arrangements might exist, which the federal government and its agencies can set their own terms....

Gayle Harrell – Florida – Former State Legislator

I'd like to respond....

Rachel Block – New York eHealth Collaborative – Executive Director

...two points I'd like to make as an extension of this though, which I think are just insights that we've gleaned from looking at these issues here in New York. One is that on the one hand, I can see enormous advantages to having all of the federal agencies adopt the same policies with regard to this question. Let's set aside for a moment what the answer to the question is, but the concept that there would be uniform application of policy across the different federal programs and agencies, I think it would be enormously beneficial to consumers and enormously beneficial to providers, so that's one thing.

The other though is that that by itself will not control a variety of other programs, services, arrangements through which other forms of data exchange will be occurring. So no matter how robust and comprehensive NHIN Exchange may become, unless we went to the ultimate solution, which I don't think we will of saying there is only one form of exchange, and that's it. I don't think we're getting there any time soon. So what we see, just in a state like New York, and I'm sure this is typical of many other places, is a multiplicity of both federal and state program requirements that are being implemented by

different components within our state government, none of which are using the same policies, and which represent not only enormous duplication of effort and resources, but which I don't think when you add it all up really constitutes a very effective approach to consumer protection or public trust.

I'd like to just – I guess a way to summarize that is, I think that there is a legal dimension here that we need to explore. I think there are some business partnership dimensions that we need to explore, but I also think that, at the end of the day, it might be very helpful for us to rise above some of the details of this and see if we could reach agreement on some kind of a broad policy construct that would lead us to greater standardization and uniformity of whatever policies are going to apply in this area.

Gayle Harrell – Florida – Former State Legislator

I'd like to respond to that. I think that business practices and business policies can't preempt state law, and you can't, for instance, if NHIN Direct says that you must allow patients to have access to lab data before the physician has released that to the patient, that is illegal in the state of Florida. Whatever their policy is, there's no presumption of state law.

Deven McGraw - Center for Democracy & Technology – Director

Can I interrupt here? This is Deven. May I suggest that the question that we're actually trying to address is not who holds the hammer, but where's the nail. Not these sort of overarching governance issues that I think we're sort of straying into and that are absolutely very important to address, could not agree with everyone more, and it's complicated, and we absolutely need to do that. In terms of coming up with a national framework of policies that have some consistency, I think that's also part of what we were trying to do. But I actually think the question that we've been asked for this call today is a bit more narrow, which is sort of, where' the locus of responsibility, not the locus of enforcement in identification, authentication, and directive transport.

Paul Egerman – eScription – CEO

Yes, that was actually very helpful, Deven, because it is narrower because we're starting to talk about some very interesting and broad subjects. This is a very narrow subject. It's sort of like saying to be very specific, if a provider wants to send a message to a laboratory, to anybody, an electronic message, who is responsible for making sure that that laboratory is the right – that the destination is the destination that's intended, and that destination is authorized to receive the message. Who is responsible for that? Is it the provider? Is it some governing body? Is it the HIO? Who is responsible to make sure that the message that the provider is sending is going to somebody who is authorized to receive it.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

This is John Houston. I think that when you scale this up to the level really this intended to go to, the provider is ill equipped to be able to perform that, and I think they need to rely upon some – again, I'm going to go back to the idea of governance or governing body that can credential, can say yes. This is an entity in good standing, and you don't have to rely upon or worry about the fact that your sending a transaction to them. That's the first point. The second point is, by the way, when we're dealing with the national roll up here, you also talk about really interstate commerce issue, and I think there is a right to have a central authority.

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

This is Dixie Baker. To real specific, and I'm not sure we even have this authority, but I, for a long time, wondered why, since HIPAA calls for a national provider identifier, why whoever issues the national provider identifier isn't also the certificate authority for those providers.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

As long as we'll provide the other services as well and the other governance stuff, I think....

Deven McGraw - Center for Democracy & Technology – Director

Yes, but why do they have to do the whole kit-and-caboodle, John? Why can't they be accountable for the function of identification and authentication?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

I think you're right. They could be. I'm just afraid that if you don't have all of those things, I'm just a big fan of trying to solve all these problems. I just see them all being incredibly important. That's the only....

Deven McGraw - Center for Democracy & Technology – Director

Yes.

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

But, John, do you see any reasons why it shouldn't be the same entity that does the management of the NPIs?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

No. No, I don't. But they need to be willing to take on these other responsibilities. By the way, maybe you could bifurcate some of this. Maybe part of this goes to a Jayco type of organization for certification, but there still needs to be an enforcement arm, and maybe you could roll that up to ORC and expand their responsibility. But somehow we've got to put something together where there's clear lines of responsibility and delineation.

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

Maybe I'm assuming too much, but I thought whoever issues the provider identifiers would have to already be doing some sort of validation that they should be given an identifier. Is that not true? I don't know. Who knows about that?

Rachel Block – New York eHealth Collaborative – Executive Director

Dixie, this is Rachel. My limited understanding of this in the last couple of months is that it's not at all straightforward. But I guess my only point just to go back to my earlier comment was simply that I just think that we need to be clear about, in answering the question, which is a deceptively simple question that Paul posed. What is our authority? I'm going back in a way to agree with Gayle. What is our authority to put some boundaries around the answer to that question?

If we're answering that question for the purposes of NHIN Direct, that may have no impact whatsoever on many other kinds of different policies and organizations. My only point was that we need to be clear about the breadth of the authority that we're trying to announce here, and if it isn't comprehensive or a single national strategy, which is kind of the direction that Dixie is going in, I just think that we need to recognize that you could come up with one answer for NHIN Direct, but you're going to end up with different answers to these questions for other purposes, and I'm just a little bit concerned about how that plays out in terms of both burden and the effectiveness of the policy.

Paul Egerman – eScription – CEO

Those are excellent observations, Rachel. I appreciate that. I actually also appreciate your other comment about the importance of getting federal guidelines and policies to help the states on a lot of these issues. I've been getting a lot of feedback from vendors who are very frustrated that a number of states are putting together privacy policies that are just different. It makes it hard for them to national organizations because there's the thing that's being perhaps over-regulated. Those are helpful things.

I'm also sensitive to what Gayle said is this is what states and even, in some cases, local jurisdictions, counties feel is important to do. But it seems like we're hearing a number of things. We're hearing Gayle say the states should do this. We're hearing John Houston and perhaps Dixie saying this should be like a centralized federal function.

Again, when I say this, I'm talking about society. Who is responsible for who has authority? I'd like to put forward a different answer, which was in my e-mail trail, which also speaks a little bit to what John has suggested about whether or not physicians can do this. But to me, the way I approach this issue is, I said, well, any time you're dealing with privacy of health information, the whole discussion has got to start with the patient and his or her physician. That's what the thing is all about. This is an interaction between a patient and a clinician and the expectation by the patient is the clinician is going to keep that information private.

The way I'm looking at this is where the responsibility for keeping it private really should be is with the provider. That the provider is the one who has got to be sure that if he or she is sending information to some other place that that is an entity that is authorized to receive it, that that recipient really is the correct recipient, and that that's really the provider's responsibility. However, it's also something the provider can delegate.

The provider can say, well, I'm responsible for doing that, but I'm going to sign a contract with my local HIO, and they're going to take care of it for me because I can't possibly do this myself, or I'm going to sign a contract with a vendor. Or maybe they say, I'm going to sign a contract with another provider. So they're located in Pennsylvania. They say I'm going to sign a contract with UPMC because UPMC is going to be responsible, is going to ... my information exchange transactions at UPMC. UPMC will take care of it and making sure it goes to the right place.

Joy Pritts – ONC – Chief Privacy Officer

This is Joy. I have a question, which is, at least in the generic NHIN Direct model, there was some, I believe there was some assumption that this would be some exchange between entities that already know each other, right?

Paul Egerman – eScription – CEO

Right.

Joy Pritts – ONC – Chief Privacy Officer

Does that affect this discussion at all?

Paul Egerman – eScription – CEO

In the proposal I'm putting forward, it's consistent. In other words, it's a great question, Joy, because it could be a situation where maybe an example, I saw a friend of mine who is a cardiologist over the weekend. He practices at one hospital, Emerson Hospital. His office is actually at the campus of Emerson Hospital, and so he just wants to exchange data with Emerson Hospital. His practice exchanging data with Emerson Hospital where the two parties know each other. It seems to me, you don't need a federal or state government to do anything.

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

This is Dixie Baker. I think his question has to do with who issues the certificates that are used for this guy to authenticate himself to another guy that he already knows. There are two levels. There's one – does this person really – you know, should I really be sending this information to this doctor? That I

totally agree is the sender's responsibility. But at the second level, which I think is the nature of his question, is who is responsible for issuing the public keys that these people will be using, these people and institutions will be using to prove that they are who they are, and that's what I was really talking about the provider. I think he's asking about that certificate authority function.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

I think it's more than that. I mean, come on. I think, once you roll up to a national, I don't think it's possible for providers to be able to do all of the things that is being advocated being done to insure that transactions that are passed are appropriate. There has to be a way that you manage this in some type or orderly, centralized fashion, or else it's all going to break down.

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

That's what the certificate authority does.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

That certificate is simply that once you've decided that that organization is entitled, I mean, it's an authorized organization, but there's also this qualitative issue here too, which is that is that transaction really appropriate, like trusted organizations?

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

Yes, yes.

Paul Egerman – eScription – CEO

There's all sorts of issues, but getting back to Joy's question ... answered it, I gave the example of a cardiologist who practices at one hospital. In some sense, a cardiologist has done its due diligence. He knows the hospital, and he has good reason to send data back and forth. Every now and then, he has to admit a patient, and every now and then a patient is discharged, and he needs the information in his medical record, and vice-versa. It meets all the criteria, and why do you need to have a national government or the state government involved? Why can't they just get certificates from VeriSign and do their thing?

David Lansky – Pacific Business Group on Health – President & CEO

This is David Lansky. Can I get in?

Deven McGraw - Center for Democracy & Technology – Director

Yes. Go ahead, David.

David Lansky – Pacific Business Group on Health – President & CEO

I've raised this a few times, and certainly it's present in the California HIE debate right at the moment. I think the natural solution, I guess, is hierarchical and that there is a top-level certificate authority or registrar at the national level, which may just simply register states. It's the next level down, at least that's the current reality in the HIE rollout. And in the California case, once California as a state or state designated entity has a certificate issuer, we're calling it an entity registry, so there's going to be a registry in California. Every entity is a trusted part on the network.

One question is, how will California set criteria for who can be in the registry. So in a sense, in my scenario at least, there may be a federal level of outer guardrails within which California can say, okay, we're going to now have entities, and we know what the outer guardrails are. Now we, California, are going to set some inner guardrails as to what it takes to be a qualified entity. The entities, in turn, can issue certificates to individual providers or sub-networks that they want to, so as you go down that

hierarchy, down to the lowest level of the cardiologist at Emerson, within the Emerson campus, maybe it's ... firewall or enterprise level boundary, they can do whatever they want internally to authenticate and manage users and access controls, but the main concept I want to add is that there's a hierarchy here of federal, state, enterprise, and maybe some sub-networks.

Deven McGraw - Center for Democracy & Technology – Director

Hold on. Let Paul finish and then, Gayle, you can go.

Paul Egerman – eScription – CEO

IN the hierarchy, David, I'm trying to understand how it works in California. Can an entity be like Kaiser?

David Lansky – Pacific Business Group on Health – President & CEO

Yes.

Paul Egerman – eScription – CEO

And issue certificates?

David Lansky – Pacific Business Group on Health – President & CEO

Kaiser may have 3,000 users, and we, in California, don't really know or care. We have some rules as to what it takes for Kaiser to be in our club, and Kaiser has to guarantee it's going to perform in certain ways and follow certain policies and not let bad actors in and punish bad actors who appear. But there is a set of rules for a Kaiser like entity in order to itself be listed in the statewide registry. But I think the specification of what's the job at each level of the hierarchy is something we could try to articulate, and it would be really helpful to the states to know what their job is and then any guidance or best practices that we could give them that they would then push down through their own structure.

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

Paul, this is Wes.

Deven McGraw - Center for Democracy & Technology – Director

Yes, and also Gayle was in the queue, Paul.

Paul Egerman – eScription – CEO

Go ahead. Who was next?

Gayle Harrell – Florida – Former State Legislator

I think Gayle is next.

Deven McGraw - Center for Democracy & Technology – Director

Gayle is next.

Gayle Harrell – Florida – Former State Legislator

David hit the nail on the head, and that's what I've been trying to get in to say is I think you've got to have, you have to have some guidance set and some guidelines set on governance structure coming out of the federal government because you do have dollars. We have dollars invested that are coming down to the state. The states need that guidance, and certainly California is ahead of the curve because they've been doing this for some time. However, it's the states that deal with credentialing with licensure for doctors for laboratories, hospitals.

A whole variety of providers out there are all licensed and credentialed under the state so that the natural hierarchy is federal guidelines coming down to states, state HIEs and states because of the dollars attached to it, and then the states have got to be the ones who really are going to set the parameters down to the HIEs and to whether it's a local HIE or a vendor HIE or whatever. You have privacy laws that are very different state-to-state. You have functional lab results laws that are different state-to-state. So you really need to set those guardrails at the federal level, and then to the states, and then let the states really develop it within the state context down to the local HIE.

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

Paul, can I speak?

Deven McGraw - Center for Democracy & Technology – Director

Yes, go ahead, Wes.

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

I'm having a difficult time deciding whether this is a discussion that is running anti-NHIN Direct or oblivious to NHIN Direct. But those two seem to be the only possibilities I can think of. NHIN Direct is formed on the premise that there is a level of communication that can be established along an endpoint that does not require a national hierarchy to be organized and in place to enable it. It asks a specific question about are there ways of assuring the issuance of the electronic credential for secure communication is within policy, but it is not. And I don't hear us addressing the question of whether all policy, all exchanges have to follow this national hierarchy, or whether there is a level of descriptive functionality associated with NHIN Direct that might make another solution practical. And I would hope we get to that point.

Joy Pritts – ONC – Chief Privacy Officer

This is Joy. I'd like to follow up on what Wes said just briefly, which was I had a somewhat – I guess this conversation is, I think, first of all, very important to have and we need to have it. I thought that Arien was starting from a different point, not that we don't want to address what you're talking about, but he was starting from a different point, which was more practically oriented, I thought, which is between – before you decide, overall, how you're going to issue the certificates. Who do you think should hold them? It's a slightly different question, I think.

Paul Egerman – eScription – CEO

It is ... actually, I don't think that's what he was asking.

Joy Pritts – ONC – Chief Privacy Officer

You don't think that's what he was asking.

Paul Egerman – eScription – CEO

I think he was asking very specifically when you said who holds the trust. Maybe he was, but I thought it was who holds the trust was really who is responsible for issuing it.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I mean, who holds the certificate wouldn't be that difficult to answer.

Joy Pritts – ONC – Chief Privacy Officer

I think that's his question, frankly, from talking to him, and I'm desperately trying to find some e-mails here.

Paul Egerman – eScription – CEO

It's a separate related question that Micky raised too, which was, that's more of an issue of granularity. In other words, who gets the certificate? Does UPMC get the certificate or does he need 3,000 certificates for all 3,000 physicians at UPMC? I got the number too low, but ... thousand physicians at UPMC, whatever the right number is.

Joy Pritts – ONC – Chief Privacy Officer

I think what Arien was trying to address was whether the intermediary, the HIPS, as they are calling them, should hold the certificate or whether the certificate level should be pushed down further to the provider. Dixie, have you been in on those conversations?

Deven McGraw - Center for Democracy & Technology – Director

Or Wes. Wes is on the....

Joy Pritts – ONC – Chief Privacy Officer

Excuse me, Wes, yes.

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

Yes, I'm here. Both of those conversations have taken place, who should hold the endpoint certificates and who should be the – they call it the anchor. That's the model that they've had to ... anchors, and it hasn't all been hierarchical. It's more a network approach.

Deven McGraw - Center for Democracy & Technology – Director

Go ahead, Wes.

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

I wanted to wait until you were finished, Dixie.

Deven McGraw - Center for Democracy & Technology – Director

I'm sorry. I thought she was. Dixie, my apologies if you weren't.

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

Yes, I am. I am.

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

I'm sorry. I think Dixie stated it well. I would just want to add that there are two frames of reference associated with the NHIN Direct discussion. One is a shorter term one where the assumption that the organizations or the people know one another and, therefore, are not relying on external mechanisms to determine whether this is an appropriate organization to exchange with.

Joy Pritts – ONC – Chief Privacy Officer

Wes, can I stop you right there? Can you give us an example to make this real for people, please?

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

Sure. Paul's example is the cardiologist who wants to exchange information with, I think he said, Emery.

Paul Egerman – eScription – CEO

Emerson.

Joy Pritts – ONC – Chief Privacy Officer

Okay.

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

Emerson, okay, and I would add the primary care provider who is doing the referral this week to a cardiologist for a treadmill test, okay, and so forth. There's many. We know right now that there are many such communications that go on without a formal organization that is validating the correctness and appropriateness of the endpoint of communication.

Paul Egerman – eScription – CEO

Not to interrupt, Wes, but to give you a couple more examples is the healthcare reform legislation has concepts relating to accountable care organizations and medical homes, but both those concepts imply relationships among a certain number of providers that exist going forward, and one could imagine that they formalize those relationships because they're transferring data frequently among themselves.

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

Right. However, in the NHIN Direct approach, there is an explicit assumption that the responsibility to reply to an inquiry about data implies more stewardship responsibility than is required just to send the data to someone for all the reasons that this committee understands very well.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

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

The second question that I think is on the table, but is not as immediate, is what are the limits on scaling this approach up to the point where it is still a transmission of data or implied consent, but the organizations don't actually know each other. And if I could give an example, that would be a mother takes her child to the emergency department for an episode of asthma and asks that this information be sent back to her pediatrician or the specialist who is treating the patient back in their home state, which is maybe across the country. Right now, there's little problem faxing that if you can get the fax number, but is there a way short of a national hierarchy to be able to make that same communication in a format that would support structured data?

Paul Egerman – eScription – CEO

In a sense, I've listened to you. What you're saying is maybe there's going to be on this whole issue of authenticating or credentialing, which is really authenticating the sender and receiver. There are really two models. There's a model where the participants know each other and communicate frequently. That's model number one. Model number two is they don't know each other as well.

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

Yes. I would say the specifics are in the characteristics of the bad actors that can come into play. If I'm doing my third referral this week to Dr. Smith, there is no doubt that I know who Dr. Smith is or anything like that. But there could be bad actors if somebody got on the Internet and stole his domain address and so forth, and there are solutions in the NHIN Direct approach to dealing with.... If it's across the country, I need to go to some directory in order to find out what's in that address for a doctor across the country there, and that implies a new level of trust and a new level of bad actorship that could come up. So it really is, does there need to be a directory or not, I think, is probably the distinction between the two cases. And if there is, what are the policy issues around a directory that just says here is the information you need to – what we're really doing is providing the information necessary for authentication and encryption, which is what the digital certificate provides. And the question is, what is the level of trust needed to have a different kind of intermediary, a directory intermediary for that?

Deven McGraw - Center for Democracy & Technology – Director

Or even, I mean, who issues these certificates, Wes, if you don't mind me getting us a little out of this? I think the directory issue is an important question, but even down. Let's take on the number one category where they actually know each other, like who do we ... issuing these...?

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

Yes, the first question that I think, beyond having problems, because Arien posed the question in a way that he thought would be most productive to the committee, and I'm trying to relate it to what's going on in the committee, in the NHIN Direct committee.

Deven McGraw - Center for Democracy & Technology – Director

Right.

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

But the first question is what is the level? What policy issues go into determining whether I can trust the group through the Internet to this doctor that I already know is valid? And is it just that we trust the Internet? I don't think so. Is there a different level of trust that is necessary? The very short-term solution is not very scalable, which is sort of out of band transmission of visual certificates. That's the first question.

Rachel Block – New York eHealth Collaborative – Executive Director

This is Rachel. I have a kind of basic question for Wes or anybody else who has been participating in the NHIN Direct discussion, which is, this concept of a provider who "knows" another provider, I'm having a little bit of a hard time getting my arms around this. I've, just in routine course of primary care, some follow up tests, etc., have recently seen five or six different providers. They happen to practice within a common organizational structure ... the name, so you can get the concept here, Prime Care Physicians. It's a very big network here in the Albany area.

What does it mean for one of those providers to know another? This is an exact replica example of the NHIN Direct world of this so-called simple exchange of information for one referral purpose or what have you, one lab result. But what do we mean when we say these people know each other? And how do we actually factor that into – how could that possibly be a building block from a policy perspective of what an appropriate set of policies around trust and security could be built on because I just don't understand what that means?

And if the knowing part goes back to the question of the directory and that, I would select. My doctor would click on the other doctor's name on the directory and, through the secure messaging, that message would go from my doctor to that doctor, but without any real knowledge of whether that doctor is in fact the person who receives it on the other end, let alone whether she actually knows, as I think you were suggesting, that that address in the directory is in fact the correct one for that doctor because that doctor might have stopped practicing or might be on vacation, but somebody else is checking his inbox kind of thing. Could somebody just tell me a little bit more about this concept of people who know each other and how we're supposed to think about that from a policy perspective?

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

Could I say something, Deven?

Paul Egerman – eScription – CEO

Go ahead.

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

I'm not sure how closely affiliated these physicians were, but let me give you my own experience. I was ... surgery about six years ago. My primary care physician in California has never been in a physician association. Most of my preop workup was done by other members of the IPA that are in fact separate businesses, separate practices that have the business affiliation. Some of the preop workup was done by doctors who aren't in the IPA and all of the material went to surgeons at Stanford who had other work done in Stanford. Of course, that doesn't matter because that's all Stanford.

What did they do? They faxed. How did they know o fax it to this place? Because they had the fax number. How did they know they had my consent? Because I signed a HIPAA consent for TPO. The question that NHIN Direct is really asking is, is it the case that policy precludes using any communications mechanism, except fax, because of threats to privacy or misidentification and so forth, or is there a level of constraints on that communication that makes some other communication mechanism besides fax feasible without a national hierarchy in place and operating?

Paul Egerman – eScription – CEO

Thanks for your comment. Let me make sure that Rachel's question is answered. I think that was your comment that there are many situations where provides have existing relationships. I gave the example of the cardiologist who practices at a single hospital. There are situations where the primary care physicians have a relationship with one or two hospitals, or they admit patients, and they have sufficient volume that they're sending information back and forth all the time because a lot of the examples is an example of a physician group who sends their labs, laboratory stuff to a single laboratory, and so that's, you know....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Paul, this is Micky here. I would even aggregate one level higher and say that UHEN and NEHEN are sort of institutionalized examples of or forbearers of NHIN Direct to the extent that all the participants in those are know to each other, and that's why they've joined in a set of bilateral relations that are put together by a switch.

Paul Egerman – eScription – CEO

That's right, and in some sense, you even broaden the concept, which is what you said, Micky. That's part of the NHIN Exchange where participants are signing a contract. They know who else is in the exchange. It's almost like a country club. They're limiting who can be in the club, and you decide who can be in it if you're willing to abide by the rules. And so it's....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes, but I was talking about NEHEN and UHEN in Utah.

Paul Egerman – eScription – CEO

That makes sense. The reason is, let me get back to Rachel's comment. The only reason the public policy implication in this that I was trying to pick up from what Wes had said was, as we look at even this narrow issue of credentials, which is who is responsible for issuing certificates. I was listening to some of the things like David Lansky was saying, which sounds very appealing, but then doesn't seem to work in a lot of the NHIN Direct environments. It occurs to me that the way to approach this is to say there are two models. There's the models where there is some direct relationship between the participants reflected in the form of contracts or we can define what a direct relationship is, but it's a direct, existing relationship that involves frequent communication. Then there's the model where the parties sort of know

each other a little bit less, and there's still a need for communication. There's a greater need for authenticating who the other player is and greater concern.

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

Paul, can I just suggest that the difference there is one is literally just authenticating that I've got the right endpoint.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

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

And the second is providing some level of credibility that that endpoint is actually a legitimate receiver of this information.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

Right.

Deven McGraw - Center for Democracy & Technology – Director

Yes, I agree with that. This is Deven. And I also think, you know, what we're trying to do here is, I mean, to Rachel's point. There are much bigger issues to resolve with Wes' second example, and we absolutely need to do it because obviously there are some limitations to a universe where the degree of trust that needs to be established is just have I got the right endpoint. I already know this person, and I want to exchange data with them, and that would be quite limited. And if we stopped there, from a policy matter, we would definitely fall short of creating the sort of bigger capital T trust framework that's needed in this space.

But in terms of the very simplistic, not simple, but maybe more simple, relatively speaking, model where there are entities that know each other, and they just need to be assured that when they send the message, it's getting to the intended recipient. I think that's the sort of small universe of sort of policy that we're grappling with, right?

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

I think so.

Deven McGraw - Center for Democracy & Technology – Director

Not to say that we don't need to address the other issues, which I think we do, but not necessarily on this call, right?

Rachel Block – New York eHealth Collaborative – Executive Director

I guess, Deven, just to close the loop, I just want to register just sort of a general concern or question about this concept of people who know each other versus people who don't know each other. I just think that if we're going to try to communicate this in a little bit of a more formalized policy context, even for the "simple" NHIN Direct functions, whether somebody knows each other or not, it doesn't seem to me a particularly relevant question. You could be sending a lab result to somebody on a patient's request. The patient might know them, but the doctor may not. I'm just having difficulty, this concept of people knowing each other or not knowing each other just doesn't make a lot of sense to me as a way to think about how to construct policy.

Judy Faulkner – Epic Systems – Founder

I agree with you. This is Judy, and it could be simply someone who is in the agreed upon list of people you can refer to that have been authorized by your healthcare organization, and often, of course, you're not sending it to that person directly. You're sending it to their assistants, who will be getting it and working it and then getting it to that person, just like it would be if it was a fax.

Rachel Block – New York eHealth Collaborative – Executive Director

And if it so happens that that person isn't taking new patients right now or what have you, we all know hundreds of different scenarios of how these things actually work out in the real world.

Judy Faulkner – Epic Systems – Founder

Right.

Rachel Block – New York eHealth Collaborative – Executive Director

In a way, it does sort of beg the question of why don't we think about this a little bit more in the fax world, but I don't want to go down that particular ... hole. But in terms of this message that's sent to Dr. X, who you thought you knew from a referral relationship, may end up with Dr. Y because of an internal organizational decision within that practice that the sending physician has no knowledge of whatsoever. So should we really be holding the sending physician accountable for what happened when that message got to that organization and ended up with somebody else?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

But that all goes into the black box that each individual organization needs to put in place to insure that then downstream access is appropriate because large organizations or hospitals, say, for instance, many people are going to have to touch that information in order to provide care. There could be transition of care, you know, a person moving from a hospital to a long-term care facility. Many people are going to see those records, and it's not going to be apparent on the surface which one of those people are going to touch the record when it's sent. But the assumption is that they have to have internal processes in place in order to comply with HIPAA that dictates that only access should be appropriate or by those people that need to see it.

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

I think we can tune up this notion of know each other, this metaphor of know each other, quickly with good effect. The first thing is that as the decision to send or receive the information is incumbent on the organization that the provider works for. It may be in some cases a sole doctor practice, but even there, that organization has an assistant, probably, or it may be Stanford that the degree to which they know each other is the degree to which they believe without further explicit verification that their transmission of the information will be for purposes they have consent, which is often treatment, payment, or operation. And I would say that rather than shy away from looking at that, we ought to explicitly look at it because I think that it sort of sets a boundary for this kind of discussion. I wrote a blog about it about six months ago trying to compare messaging to fax and finding that fax was actually pretty functional....

Paul Egerman – eScription – CEO

I read your blog, Wes. It was interesting.

W

Can I just say one last thing? Just go back to one of the points we were chewing on a few minutes ago, part of the reason that this provoked a thought line for me was when we talk about what the physician is

responsible for. I just think that we need to be clearer about the boundaries of that physician's responsibility as it relates to what happens.

If they've made a good faith effort to communicate that information to the person they thought they knew, that we somehow capture that as part of our policy scheme. And the fact that that information may end up in that other organization with somebody else entirely shouldn't be that physician's responsibility. But that that organization then has a responsibility to make sure that the appropriate certificates and so forth are in place in a ubiquitous way across that organization. It does tie in a little bit back to the earlier point, I think, and I just think that we need to be a bit crisper about what we think specifically the physician or the provider is responsible for.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Judy Faulkner – Epic Systems – Founder

Are we taking this to too granular a level? Shouldn't it be that every organization that participates in this has got to agree that they will treat everything appropriately and you don't have to know them? It just has to be wherever you send it, you know you've sent it to someone who has a legal agreement that they will treat it appropriately.

Paul Eggerman – eScription – CEO

Legal agreement with who?

Judy Faulkner – Epic Systems – Founder

In California, it would be with the California group that is saying these are the rules and this is how you have to do it.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Judy, this is Deven. I think ultimately that gets to one of the reasons why we're sort of pursuing on two tracks here. There is a sort of framework position, framework set of policies, some of which are already reflected in law, some of which may be better expressed because they're not well reflected in law in terms of data sharing agreements, but that the people generally commit to complying with the law and a responsible set of data policies, so that is absolutely foundational.

But in terms of, I think I heard Rachel's point as being the law, actually, quite frankly, might otherwise hold an individual physician responsible for when they share data and who they share it with. And to the extent that that puts some of these – it puts providers in a difficult position because they don't always know how that information is going to be handled, notwithstanding that everybody should be committed to following good data policies, that we just need to be clear about sort of where those obligations lie.

Judy Faulkner – Epic Systems – Founder

Okay, as long as it's trying to make sure that we don't get the providers with the best of intentions trying to make sure that if I have to go quickly somewhere, and they don't know enough about that organization to know individuals in there, but they know I have brain trauma, and they don't know any....

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Judy Faulkner – Epic Systems – Founder

That they will get me there right away without having to worry about their own liability or go through a lot of processes.

Gayle Harrell – Florida – Former State Legislator

This is Gayle. I'd like to jump on that a minute. I think also you want to be careful that we don't open up more doors of liability for physicians or providers that, in the long run, is going to be a very negative thing in moving forward with adoption. You start opening up a whole new level of liability, you're going to create many, many more problems than you're even anticipating.

Paul Egerman – eScription – CEO

Good comments. Let's go back to the original question. The question was who holds the key to the trust level.

Deven McGraw - Center for Democracy & Technology – Director

Everybody.

Paul Egerman – eScription – CEO

The HIO or the provider? What are we saying the answer is?

Deven McGraw - Center for Democracy & Technology – Director

And so, but let's, Paul, if you don't mind my interrupting, I think we should be clear what we mean by trust. We're talking about the identification and authentication piece of trust, right?

Paul Egerman – eScription – CEO

That's right.

Deven McGraw - Center for Democracy & Technology – Director

Which is just one component of trust.

Paul Egerman – eScription – CEO

Right. What's our answer to that question based on this discussion? In other words, who issues the certificate? Who is responsible for making sure that the players who have one are the right ones, and who is responsible for that?

Deven McGraw - Center for Democracy & Technology – Director

Can I try?

Paul Egerman – eScription – CEO

Yes.

Deven McGraw - Center for Democracy & Technology – Director

This is Deven. There absolutely needs to be some responsibility and clear policies for certificate issuers. It's not clear to me at this point that it needs to be a centralized function necessarily of the federal government or even necessarily of state governments, but it needs to exist, and it needs to operate with a clear set of policies and a mechanism for holding entities that issue those certificates accountable. There is the possibility of doing this in a decentralized way, but only in accordance with some clear policy, and that assumes that there will actually be organizations that will rise up to meet that functionality. And if it doesn't exist, then it may need to be provided by government.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Deven, this is Micky. The example of decentralized would be that I'm an intermediary. I say you can, as a participant, you can go and get a certificate from VeriSign, RSA, whoever, or we could do a list, versus, and the converse, the centralized is you can only get certificates through me.

Deven McGraw - Center for Democracy & Technology – Director

Yes ... see what I'm saying.

W

Yes.

Paul Egerman – eScription – CEO

Based on what you're proposing, picking up what Micky said, Micky listed like VeriSign, RSA. Those are the organizations that meet the federal guidelines.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

You're going to have to have some authorizing body that authorizes the certificate authorizers.

Deven McGraw - Center for Democracy & Technology – Director

I may in fact be suggesting that. I mean, there is, getting to John Houston's governance comment, I think if we're going to say to providers we think it's unfair to hold you individually responsible for whether or not you're sending to, you know, if you intended to send to Dr. Brown, whether it gets there or not, and we think that there are trusted parties in the middle who can assist, but we want to make sure that they comply with certain criteria, we think government has a role in setting those criteria. I think that's what I was hearing. Then how do we get that enforced? Is it through a set of government rules? Is there a role, for example, for accreditation? This is a sort of straw dog proposal that I'm going out there.

Joy Pritts – ONC – Chief Privacy Officer

Right. This is Joy. I keep hearing this word "governance", so I'm getting a little, you know, this is one of our ongoing is, is NHIN workgroup represented on this call, and are they addressing governance issues?

Deven McGraw - Center for Democracy & Technology – Director

We have no idea.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

I've never heard of anybody stepping up about governance.

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

It's my understanding is that the NHIN workgroup is addressing governance issues for NHIN Exchange. I don't know that anyone has stepped forward and identified itself as an entity for NHIN Direct or said that the NHIN workgroup should, as a matter of fact, be the policy organization for NHIN....

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Can I also suggest that the NHIN – what I'm hearing or sensing is that their idea of governance is incredibly limited and is to setting the standards and doing nothing more.

Deven McGraw - Center for Democracy & Technology – Director

No, that's not what I said, John. What I'm trying to do is to – I actually, I don't necessarily want to get to the question of who governs or even necessarily how yet, but rather to sort of lay out a set of policies that we say need some governance infrastructure and parking lot for later consideration, whether it's by us, by NHIN workgroup, I don't know.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

I agree. My point was only the question that was asked about what are they don't, and my understanding of reading was that there was a very limited idea of what governance should be, and that's my only point.

Joy Pritts – ONC – Chief Privacy Officer

I just wanted to make sure that we weren't going to be – I just wanted to make sure we were coordinated.

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

I think the question of what....

Deven McGraw - Center for Democracy & Technology – Director

We could ... from you guys actually in that regard.

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

The question of what governance is and whether it needs to be all encompassing, or it's not in use is, I think, a legitimate question....

Paul Egerman – eScription – CEO

I think it is a legitimate question. I have this sort of determination though to answer this question. I think we can deal with the governance issue in separate meetings and calls. The question that was actually said, who holds the keys to the trust level, which a variation of that is who issues the certificate, and I heard Deven put forward a proposal, which was, it's decentralized, and you're going to have these things. I don't know if anchors are the right words, but organizations that are able to issue the certificates based upon federally established rules. I suppose the states could add additional restrictions if they want, but those are the organizations that will do it, and that's a decentralized model. My question is, is that an answer? Is that an answer we're happy with? Is that ... answer?

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

I have to ask a question, which is, is that organization responsible for vetting the identity? In other words, right now, in one of the services that the typical HIE provides is to assure that this thing that's called Joe's Endoscopy Shack is or is not a provider before it'll let it into the club? Is that what we're expecting of this entity that you're describing, Deven?

Deven McGraw - Center for Democracy & Technology – Director

Yes, I think so.

M

Yes.

Paul Egerman – eScription – CEO

Although we could clarify that in our answer to the question is that's one of the things these organizations will have to do.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egerman – eScription – CEO

We say that's part of our answer to the question.

Latanya Sweeney – Laboratory for International Data Privacy – Director

This is Latanya. I have a question. There are a couple of vendors out there who have a slightly different model that's very interesting. They are based on the federal government's guidelines that would require two-factor authentication, and so they basically leveraged the two-factor authentication model. It primarily is in hospital systems where you can pull this off, along with the fact that where the person is located in order to authenticate them. And so that if the data was communicating across a network, that they don't actually need further authentication, only the approval of the hospital system. That's a situation. It's an interesting – I'll put it out there. My job is to give you examples that keep you broader and without over-fitting.

Paul Egerman – eScription – CEO

So are you saying that this is a question we shouldn't have to answer? You say that there's a way to do this without a certificate?

Latanya Sweeney – Laboratory for International Data Privacy – Director

There's a way to do it without having global certificates, yes. There's more than one way. In fact, there's at least five ways that I know of.

Paul Egerman – eScription – CEO

Wow.

Deven McGraw - Center for Democracy & Technology – Director

Yes. In other words, we should not be confining our recommendations to the issuance of certificates with certificates as one mechanism for assuring identity, but there are others.

Latanya Sweeney – Laboratory for International Data Privacy – Director

Yes, that's my point.

M

Right, and I think Arien's question was trust, right? And he put that in quotes.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Ultimately, you could say, look, the reality is that typically, as a concept of data stewardship, when you're sending data out, you do have some responsibility to make sure that it's getting to the right place, but there's a limit from a policy standpoint to what an individual doctor, much less even an institution, is able to do without some help in that regard, in most circumstances. And so to the extent that there is that need in the middle, who serves in it? And does it need to be some centralized authority, or can in fact it exist in multiple ways as long as it meets certain specific criteria?

Joy Pritts – ONC – Chief Privacy Officer

This is Joy, and I have finally found my – in this vast amount of e-mails – some of the e-mails from Arien. You're addressing this issue at a very high level, which I think is good, but I'd also like to challenge you to address his issue that he's raised, which is a little bit different. If we can turn to that before the end of this call since I think we're kind of winding up here, right?

Paul Egerman – eScription – CEO

Right.

Joy Pritts – ONC – Chief Privacy Officer

He had somewhere here, whether, let's see, whether the key should be held closer to the provider or closer to the – whether the trust level is established closer to the sender or at the intermediary level. And then he has whether he keys, the pros of it being – he had pros and cons listed as to whether it's held closely or whether it could be delegated to the HISP. That's it. His question was whether the keys had to be held at the provider level, or that they could be delegated to the HISP.

Paul Egerman – eScription – CEO

Right, and that's sort of like your question, Joy, the way I was trying to respond to that, Joy, is I said the provider is responsible, but they can delegate it to somebody else. In other words, if you have these other organizations who can do them, they're authorized to do it for them, the provider could choose one of those.

Joy Pritts – ONC – Chief Privacy Officer

Has everybody agreed with that?

Paul Egerman – eScription – CEO

I don't think so yet.

Joy Pritts – ONC – Chief Privacy Officer

Was that discussed by anybody?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Can I just ask? This is Micky. Deven, if I understood your sort of proposal, what you were suggesting is that we, in effect, not say one or the other, but we say, in effect, that if it is centralized, there'll be certain policy considerations that way. If it is decentralized, there are certain policy considerations that way, without getting into the policy is that it has to be one way or the other.

Joy Pritts – ONC – Chief Privacy Officer

Then your recommendation is, it doesn't matter as long as certain things are in place in these different areas, but that still addresses what he's asking.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes. I just wanted to make sure I understood what Deven was suggesting first, so I was correct.

Deven McGraw - Center for Democracy & Technology – Director

Thanks, Micky. It was a combination of the two, which is, yes, it's at the individual level, but it can be delegated, but does that delegation happen to some centralized authority, or can it in fact be decentralized as long as it meets certain criteria? Does that make sense?

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

Are you asking specifically about – I think, Joy, it would be a wonderful thing if you were to just rely to all and send that particular e-mail to us because I've been looking for it too.

Deven McGraw - Center for Democracy & Technology – Director

Wasn't it part of the e-mails that Paul sent out for the first meeting?

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

For this meeting?

Deven McGraw - Center for Democracy & Technology – Director

No, for the initial for Tuesday's meeting.

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

It's possible.

Deven McGraw - Center for Democracy & Technology – Director

I mean Thursday's meeting that Paul sent on Tuesday.

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

Okay. I can probably find it then. Now I lost.... I think that he's asking the specific question or that a translation of this question would be if in fact one of the services that HISP provides is maintain certificates for the edge organization, whether the policy requirements for qualifying a HISP as opposed to a more general question of decentralization. And the reason is that they're grappling with the same business issue that everybody grapples with that a large organization is qualified to get and maintain digital certificates, but a small practice isn't.

Deven McGraw - Center for Democracy & Technology – Director

Right. So they have to rely on someone else, and we want to make sure, regardless of who issues the credentials, whether it's done through digital certificates or it's done through two-factor authentication, as Latanya raised, whatever the mechanism there. Ideally what the policy would reflect is that anybody who is playing in that space has to meet certain baseline criteria, whether it's level of assurance, assumption of liability for making mistakes, that kind of....

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

Yes. So I guess the more abstract representation is header. If a third party ... for someone else, is maintaining the certificates for a medical organization, what are the requirements on that third party? I guess certificates might be too specific. Maintain the....

Deven McGraw - Center for Democracy & Technology – Director

Credentials.

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

Credentials, right.

Paul Egerman – eScription – CEO

It's credentials, but there really was a centralization versus decentralization component to this question, which is, is it the responsibility of the provider? Is it centralized? David Lansky came up with an entire hierarchical suggestion. Is it centralized, and that's how it works? Is it the responsibility of an HIO to do this? Where is the reasonability for the credentialing activity?

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

I'm suggesting that where is the responsibility. The different question Deven asked, which was more like, what is the responsibility.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

Her answer is who does it. She says you can have a decentralized group of organizations, for example, who issue the credentials, and it's almost implied if it's decentralized, then it's sort of like you're a provider, and you can choose. Just like you could choose who your auditor is or who your accountant is. You can choose who you want to get your credentials from.

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

I thought – okay. Deven...?

Gayle Harrell – Florida – Former State Legislator

...caveat on that, Paul. This is Gayle. You've got to have somebody really accrediting those.... There's got to be some standard in place. Deven made that point.

Deven McGraw - Center for Democracy & Technology – Director

I tried to make multiple points. I don't know that it was a fully formed idea, but it was an attempt to get us to one.

Gayle Harrell – Florida – Former State Legislator

I know the direction you're going, and I'm thinking in the same direction, but you have to make sure that whoever is doing the authorization of those certificates or whatever ... it has to be some kind of accrediting body. Otherwise you can get all kinds of entities out there doing it.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I don't know that I'm sort of fully aligned behind an accreditation model, but what is clear to me is that there needs to be some way for providers to be able to establish that trust in terms of identification and authentication. Some of them will be able to do it. Some larger institutional providers will be able to do it without any additional assistance, but some smaller – but other providers will need some. Does it need to be created through some sort of central authority? It's not clear to me that either we could stand one up quick enough to do it or that it makes sense to do so.

To the extent that there are organizations who can stand up and perform this service or function, I think that's fine as long as they agree to certain policies, and there's a mechanism for holding them accountable for doing that, whether it's accreditation, whether it's government regulation, whether it's BA agreement. I'm less certain of that, but it seems as though this sort of question of centralization versus decentralization is, in essence, not as much of a policy question as a question of what's going to work because, from a policy standpoint, you want to make sure that any entity that does it is held accountable for doing it correctly.

Gayle Harrell – Florida – Former State Legislator

Correct.

Deven McGraw - Center for Democracy & Technology – Director

And that, to the extent that they're gathering some data about providers and maybe individuals, to the extent that this also has to do with patient identification, that there are some rules and requirements around the personal data, not necessarily health data, but the personal data that they may collect in order to do the identity management piece of this. That's essentially what I'm saying. I hope that makes sense.

Paul Egerman – eScription – CEO

I'm looking at the clock. Let me make a perhaps futile attempt to summarize what I think Deven is proposing, and so I'm going to see if I can summarize it, and see if we can get any level of consensus

around it. One way to summarize it is to say, on the one hand, to maintain the patient/clinician relationship, it's certainly the responsibility of the provider to protect the privacy of the data. That does imply, among other things, when there's any information exchanged, they send it to the right recipient, and so that's the responsibility of the provider. But the provider can delegate that, and they could delegate it to organizations that are identified at least initially as decentralized organizations that are going to be authorized to issue these credentials under a series of guidelines or rules that are established by the federal government and which may also be augmented by state law, and which include basically verifying that the provider requesting the certificate is who they really say they are.

Furthermore, as we say all of that, this is also an issue that we may revisit when we get to the other issues like governance and directory services. This is our answer for at least this narrow question. What do we think about that summary? Is that something people are comfortable with? Am I close or far away?

Deven McGraw - Center for Democracy & Technology – Director

It sounded right to me.

M

Sounds good.

Paul Egerman – eScription – CEO

What about David Lansky, Rachel, Gayle? What do you think?

Deven McGraw - Center for Democracy & Technology – Director

Wes?

David Lansky – Pacific Business Group on Health – President & CEO

This is David. I think it's fine. I think it allows for a variety of solutions....

Gayle Harrell – Florida – Former State Legislator

This is Gayle. I would agree with it. I like the decentralized aspect of it and the flexibility, as long as they are provisions within, as we flush it out a little bit more, that really ... the accountability and the governance of it.

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

Yes. I think it's a good basis to comply with. It maybe a little bit of an agenda item too, but....

Paul Egerman – eScription – CEO

Yes. I think, at some point, there's – I'd like to say this issue is done, but there's probably a lot more to talk about on this when we dive into deeper layers of this issue. But do we feel? Is there anybody who wants to disagree with this? Is there anybody who doesn't really like it and is not really happy, or is it just everyone either agrees with it, or they're exhausted, one or the other?

M

You said we're tabling the other part of the governance issue, correct?

Paul Egerman – eScription – CEO

Yes, we're tabling it for now. In the agenda that I put forward, we actually have it towards the end in August. But governance is a really important issue because, on all these things, we have to talk about what happens with the bad players and how are we going to enforce these things. We have some

enforcement levers with meaningful use and certification. But there are a lot of other very interesting governance issues.

M

Right. I'm satisfied with that.

Paul Egerman – eScription – CEO

Pardon me?

M

I'm satisfied then overall.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Paul, this is Micky. I think it sounds okay too, but I'm speaking for me, and I suppose a bunch of others, just seeing it in writing will help.

Paul Egerman – eScription – CEO

Yes. I guess that's the benefit of this meeting being on Friday because we have, I guess that gives Deven and me Saturday and Sunday to try to write it up.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

We'll put it in writing for you. However, one of the comments ... we put it in writing, we want to avoid wordsmithing this stuff. So if you don't like the wording on it, you should just let us know and we'll do our best to accommodate you. What's more important is that we capture the concepts correctly. And so if you had a chance to look at it, and you're uncomfortable with it, that's fine. What do we do now that we've actually made terrific progress today? It's exhausting, and we've been talking for a longtime.

We actually answered the two questions that Arien asked. There's another related question that we could try to touch on briefly, which is the granularity question that Micky raised. Is this done at a provider level or at an individual clinician level? Or we could say this is good work for a long meeting and a long week, and open ourselves up for public comment. What do you want to do?

Gayle Harrell – Florida – Former State Legislator

We only have five minutes left.

Deven McGraw - Center for Democracy & Technology – Director

Yes, we only have a few minutes left. I think new can probably get to that granularity question – I could be completely wrong about this, but at least how you would address that in terms of policy, relatively easily in compared to some of these other issues. But I'm always optimistic about this stuff, but nevertheless, since we only have five minutes, in case it is as gnarly and difficult as all of the other ones we have tried to tackle, probably best to leave it to fresh heads and allow people to take bio breaks, and get on to the other things that they actually get paid to do.

Paul Egerman – eScription – CEO

First, let me ask, do any members of the team have any other comments they want to make before we open to public comments? Any comments, questions, observations, complaints? Terrific. Judy, why don't we open up the lines and see if the public would like to make some comments or questions?

Judy Sparrow – Office of the National Coordinator – Executive Director

Let's do it. Just a reminder to the public to state your name, organization, and you're limited to three minutes. Operator, if you would open up the lines, please.

Operator

We have no questions at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director

Okay.

Paul Egerman – eScription – CEO

First, let me once again thank the ONC staff people: Judy Sparrow, Joy Pritts, and anybody else from ONC who have helped put this meeting together. I want to especially thank all of the team members who stuck through a difficult meeting. Again, this is hard stuff that we're doing, and it's not easy, but I think actually we made terrific progress today, and so Deven and I will write this all up. Our next meeting is when, Deven? I'm a little confused. When is our next meeting?

Deven McGraw - Center for Democracy & Technology – Director

I'm going to ask for Judy's help on this. It's on Tuesday.

Judy Sparrow – Office of the National Coordinator – Executive Director

Tuesday, we haven't really sent anything out yet. Tuesday, June 15th, the possibly it'll just be a short call, 1:30 to 2:30, unless I hear from the NHIN workgroup that they're not using that time. So if you can bear with me until the end of the day, I will get an invite out before 5:00 today.

Paul Egerman – eScription – CEO

Terrific.

Judy Sparrow – Office of the National Coordinator – Executive Director

Then after that, the next one is on June 22nd, 10:00 to 1:00.

Deven McGraw - Center for Democracy & Technology – Director

We essentially have two more meetings for finalizing what we want to do, the recommendations we want to make to the policy committee on the 25th.

Judy Sparrow – Office of the National Coordinator – Executive Director

Right.

Deven McGraw - Center for Democracy & Technology – Director

That's good to know.

Paul Egerman – eScription – CEO

Right.

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

I think we need ... a round of applause here to Paul and Deven.

Judy Sparrow – Office of the National Coordinator – Executive Director

Yes.

W

Here, here.

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

I'm sitting here with the impression they're not even perspiring....

Deven McGraw - Center for Democracy & Technology – Director

You can't see me in my office, Wes. It's awfully nice of you. It's only because we have such great participation.

Paul Egerman – eScription – CEO

What we need to do next is really focus on these framework documents.

Deven McGraw - Center for Democracy & Technology – Director

Yes, thank you, Paul.

Paul Egerman – eScription – CEO

That is really the next agenda item, and so the way you could help us do that is I know some people have put forward their comments on it.

Deven McGraw - Center for Democracy & Technology – Director

Yes, but not very many. It's not at all reflective of the entire group yet because I think folks haven't had a chance to really dig into it.

Paul Egerman – eScription – CEO

Yes. It's a very different thought process. What I'd ask everybody to do is to read through the frameworks document. Read through it carefully, and to what I call redline it. Change anything you want, except what's in the first column. Change the other columns. Put in whatever comments you want because that will also expedite our discussions. If people are able to read it in advance and come to some conclusions, then we could start to race through it because what our final recommendation is going to be is on June 25th, our report for June for this month is going to be that framework document, plus the answers to these questions, which is, if we can get through that, we'll have done a huge ... this will be a good step forward in the process. Deven, do you have anything you would like to add?

Deven McGraw - Center for Democracy & Technology – Director

Yes, just in terms of what the framework, you know, there was an initial one that we distributed for, I think, the initial administrative call, and then I updated it another time. But if you want to make sure you have the most recent version, it's the one that you can download right from your screen. It says NHIN Policy Framework.

Paul Egerman – eScription – CEO

Why don't we send it out again?

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Judy Sparrow – Office of the National Coordinator – Executive Director

I'll send it out.

Deven McGraw - Center for Democracy & Technology – Director

Thanks, Judy. That's great. I just, with Paul, thank everyone for their time and attention and active participation. Really appreciate it.

Paul Egerman – eScription – CEO

We're making progress. Have a good weekend.

W

Paul, I think we need to thank both you, Deven and Paul, for the amount of work you guys are putting into this.

Deven McGraw - Center for Democracy & Technology – Director

Thanks, Judy.

M

We now know why you guys get the big bucks.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

I'm never going to live that comment down. I can just tell.

Deven McGraw - Center for Democracy & Technology – Director

Gratifying attention, that's what I'm doing.

M

Right.

W

Eternal gratitude.

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

Any attention is better than no attention.

M

All right. Thanks, everyone.

Judy Faulkner – Epic Systems – Founder

Thanks.

M

Thank you. Bye-bye.

Gayle Harrell – Florida – Former State Legislator

Bye.

W

Bye.

Public Comment Received During Meeting

1. I recommend a review of 45 CFR Part 142 Security and Electronic Signature Standards; Proposed Rule. It is a starting point to implement a x.509 addressing and PKI infrastructure. This would allow a secure, reliable, accountable communication with non-repudiation. It would only expose the content to the addressee. A x.509 address does not contain any PHI.

2. You don't have to have a BA with every ISP that transmits encrypted PHI. Why would you have to have a BA with intermediary if they do not have access to the encrypted information?