

Privacy & Security Tiger Team
Draft Transcript
October 15, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director

Good afternoon, everybody and welcome to the Privacy and Security Tiger Team. It's operating as a federal advisory committee, which means there will be opportunities at the end of the meeting for the public to make comments. 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 – Software Entrepreneur

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Latanya Sweeney? Gayle Harrell? Carol Diamond? Judy Faulkner?

Carl Dvorak – Epic Systems – EVP

This is Carl here as well.

Judy Sparrow – Office of the National Coordinator – Executive Director

David McCallie? Actually, John Travis is on for David today.

John Travis – Cerner – Sen. Dir. & Solution Strategist – Regulatory Compliance

Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director

Neil Calman? David Lansky? Dixie Baker?

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

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Micky Tripathi? Rachel Block? Christine Bechtel?

Alice Brown – National Partnership for Women & Families – Director HITP

Hi, this is Alice. I'm on for her.

Judy Sparrow – Office of the National Coordinator – Executive Director

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

I'm on for myself today.

Judy Sparrow – Office of the National Coordinator – Executive Director

Leslie Francis?

Leslie Francis – NCVHS – Co-Chair

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Joy Keeler?

Joy Keeler – MITRE Corporation – Health IT Program Manager

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Adam Greene?

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

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Lisa Tuderow?

Lisa Tuderow

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Arien Malec is on. Did I leave anyone off?

Judy Faulkner – Epic Systems – Founder

Judy Faulkner.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you. I'll turn it over to Deven and Paul.

Paul Egerman – Software Entrepreneur

Thank you very much, Judy, and thank you to the members of the Tiger Team for participating on this bright and sunny or drizzly Friday afternoon, whichever one of those that you have. We have a very interesting topic to review. My colleague, Deven McGraw, is in transit right now so I'll be doing most of the talking as we get started, as we go through the agenda. Deven has been working on setting the *Guinness Book of World Records* for the longest time to take to travel from Trenton, New Jersey to Washington, D.C. I think she's—

Deven McGraw – Center for Democracy & Technology – Director

Thanks, Paul.

Paul Egerman – Software Entrepreneur

... very close to have set the record. But she's on her way back, I understand, and probably listening on a cell phone in a cab or something.

Deven McGraw – Center for Democracy & Technology – Director

Actually, I'm seconds away from being inside of my condo, so we're all good.

Paul Egerman – Software Entrepreneur

That's great. So what I want to do is talk you through very quickly what the agenda is today. First, we're going to do a very quick wrap up on the transparency recommendation. Then what we're going to do is start framing our discussion about provider entity authentication. This is really a fascinating topic. It's actually, in one sense it's sort of like a small chunk of everything that we have to do, but it's also a very interesting topic and we're going to be spending most of today talking about background material and framing the discussion. So you'll see at the end of the agenda how it says proposed questions for the Tiger Team, but the purpose of this call is really going to be to give you some background information about this topic and to make sure everybody's comfortable with the way we're framing the topic and to find out if you're not comfortable how we need to change that. So that's what we want to try to get accomplished.

Now, we're not going to spend time today on the transparency recommendations that are listed here in the agenda. You should have received today an e-mail with what I would call the almost final version of the transparency recommendations. On Wednesday of next week, October 20th, Deven and I will be presenting that to the policy committee and so we're going to give you all just simply one last chance, if the Tiger Team members want, to make any last wordsmithing changes. I think Deven primarily did her best to incorporate everyone's changes, but if you're uncomfortable with it or it's not quite right, if you could get back to both Deven and me by noon on Monday that would be very helpful so that we can turn it around and get it to Judy and the policy committee people so they can read it in advance of Wednesday's meeting. So that's our request on transparency.

The issue that we do want to spend most of our time discussing is this issue of provider entity authentication. On this screen you see a very brief discussion of the scope of this discussion. It says that what we're trying to do is define policy recommendations to ensure that authentication and "trust" rules are in place for information exchange between provider entities or organizations. So ... description of this word "authentication." To try to make sure that we understand what this all means we're defining authentication, but when we say we want to ensure that authentication trust entity rules are in place we simply want to make sure that if one EHR system, say an EHR system at UPMC, is sending a patient summary to an EHR system at, say, Partners, that the computer system at UPMC has a sense of confidence that Partners is really the one that's getting it.

So we're defining authentication as verification that a person or entity seeking access to electronic protected health information is the one claimed. Again, to try to give you a real world example of that, since I just mentioned Deven, but if Deven should happen to place a phone call to me and I can look up my phone and I see caller ID says somebody's calling from Center for Democracy and Technology—Deven's company—and especially if I'm expecting her to call, that's one way to authenticate that I know who the call is coming from. So that's what authentication is, is knowing somehow who's on the other end. Level of assurance is also a definition of something that we'll be dealing with, sort of like the degree of confidence, how confident are we that basically the authentication is correct, that we know what is going on.

Then in terms of framing this discussion, we're going to be specifically interested in the first bullet addressing directed exchange transactions that are described in stage one of meaningful use. In doing that again we're going to be assuming that identifiable clinical information is being transmitted and we also are assuming that this is confidential information. So we're not making distinctions between sensitive data and data that's not sensitive, but it's reasonable to assume that this does include sensitive data based on some of the things we've talked about in the past is being included.

The next thing that we probably want to discuss a little bit that I want to make sure everybody understands is in terms of how we're getting started to frame this discussion is we are evaluating the trust rules at the organizational level. So sometimes you call it an entity level, but at the organizational level. The reason for that is these are basically EHR systems that have to talk to each other in directed exchange, so ... the scope does not include authentication of individual users of EHR systems.

Then you see on the slide a statement that says, "Provider entities and organizations must develop and implement policies to ... and authenticate their individual users." The reason we put that there is to make sure everybody understands that we all know that there's other stuff that has to happen from the trust. It's not just a matter of authenticating the machines, there are a lot of other things. You have to make sure that users are authenticated. You've got to make sure that the data is correct. There's a lot of other information exchange issues, so we want to make sure that we clearly understand it and we're only looking at one component of it. There's also a statement that beyond stage one of meaningful use policies ... user authentication may be needed. In other words, it depends on what we see in some of the subsequent information exchange transactions.

I have a few more things I want to go through, but let me pause a minute and find out if anything I said here people have any comments on or questions about.

Deven McGraw – Center for Democracy & Technology – Director

Thanks, Paul. I just wanted to let you know that I'm fully with Internet access and a phone without background noise.

Paul Egerman – Software Entrepreneur

That's exciting. It's also great because when I finished talking I thought to myself, I wonder if I'm still connected and if everyone can hear me.

W

I was wondering that myself, Paul. It's awful quiet today for this group.

Paul Egerman – Software Entrepreneur

So continuing on then, here are the five questions. So these are the questions the way we tentatively are framing this issue. What I'm going to do is I'm going to go through these quickly, but then what we're going to do is we're going to go through some background material for everybody and then we'll revisit these at the end. At the end of the discussion we're going to give you a chance to tell us that these are the right questions, if you like them, if we missed something, and so on.

The first question is: What strength of provider entity authentication, in other words, level of assurance, might be recommended to ensure trust in health information exchange? So this is like a key recommendation that we're making, is what is the strength? What's the level of assurance? The thing that you see in parentheses, it says "regardless of what technology," it's very important to understand we're not going to make a technology recommendation. We're not going to say to use a specific digital credential or a specific certificate or anything like that. That's the kind of stuff the standards committee is going to be doing. We're simply going to be trying to do policy guardrails. That's the first one is the level of assurance.

The second issue is: Which provider entities can receive digital credentials and what are the requirements to receive those? The third one is: What is the process for issuing digital credentials? So this gets to be very interesting in terms of evaluating whether initial conditions ... and reevaluation on a periodic basis. The fourth one is: Who has the authority to issue credentials?

The final one is written in s— It's like a mouthful when you read it out loud. It talks about: Should ONC select and establish technology? The best way to understand it is, the question is: When it comes to this concept of digital credentials and authentication, is that an area for standardization and certification? Are

we just doing a best practices recommendation or do we want to actually standardize and certify a single technology? So that's also an important issue.

That's what we think is the framing, and again, unless somebody has any questions about this—

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

Paul, I have a question. I think I heard someone else too. This could be read a number of ways and I just need to be sure that the way I want to read it is a legitimate read. There are many levels of authentication. One is ..., but two that are often used as the main points in the spectrum are authentication of an individual person and the other is authentication of an organization. The technical implications of working at those two levels are very substantial and particularly when it comes to communicating the authentication mechanism, they're very substantial. So I guess I need to ask, are we lumping those two together? Are we addressing them separately? Or are we just addressing one or the other?

Paul Egerman – Software Entrepreneur

The answer is we're not lumping them together, we're answering them separately and what we're calling entity is what you're calling the organizational level. That's what we're going to be doing right now. Then how we're going to handle individual is currently unknown.

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

So the provider entity here is an organization as opposed to Dr. Jones? It might be Dr. Jones' solo practice, but it's not Dr. Jones.

Paul Egerman – Software Entrepreneur

Exactly right.

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

I have a question as well. Regarding the work that's going on with the Governance Workgroup, it seems like some of these questions—though I agree that these are security related—do either butt right up against what I think some of the Governance Workgroup activities are trying to address, as well as the fact that I suspect, and I know this is sort of telegraphing a solution rather than stating a question, but I think that a lot of the solutions will appear at least to be ones that would be similar to solutions that the Governance Workgroup would be working on. I understand they're from a different perspective and a different framework, but nonetheless how are we going to make sure that we harmonize what we're doing with regards to these questions with what the Governance Workgroup is doing and will we try to look for common points where we can try to integrate solutions rather than having standalone solutions?

Paul Egerman – Software Entrepreneur

Those are excellent comments. You asked a number of questions and I'm not sure I know the answers. I guess part of the answer about how we harmonize and how we coordinate is we've got great people like you who are on both committees, so that helps us.

Joy Keeler – MITRE Corporation – Health IT Program Manager

We're working very closely within ONC to stay coordinated on these and check in on at least it seems a daily basis on this issue, recognizing that there is some overlap here, but with the Governance Workgroup really feeling that the Tiger Team was the one that should be taking the lead on some of these privacy and security issues.

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

Absolutely and I don't disagree. I know some of the recommendations we made as a Governance Workgroup, I think that if we start to look at the ways to be most efficient we're going to find that maybe the same vehicles will be in place for both types of recommendations I think we're going to be making.

Gayle Harrell – Florida – Former State Legislator

Gayle Harrell's now on. Sorry I'm late.

Paul Egerman – Software Entrepreneur

Hi, Gayle. I understand Micky just joined also.

Neil Calman – Institute for Family Health – President & Cofounder

Neil's on too.

Paul Egerman – Software Entrepreneur

Hi, Neil. It's great to have you. Thanks for joining. So I just want to make sure I respond to your comment, John. We definitely have an issue that we have to coordinate with the Governance Group. The other comment I want to give you, though, is that this is authentication for information exchange—

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

Oh, yes.

Paul Egerman – Software Entrepreneur

... really a narrow part. We have to be careful that we don't think this is a total solution to everything. There's tons of other governance stuff beyond this.

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

I'll give you an example. Number four, who has the authority to issue digital credentials? I would think that that is in part a result of the governance function of deciding who can participate within the network. So I just want to make sure that as recommendations remain regarding governance, that things like this, which are I think are almost a byproduct, also get harmonized and put together in a common framework.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I think that's right. Certainly, having sat in on that one hearing, and then we had the joint call last time, to the extent that you all in the Governance Workgroup are looking at maybe infrastructure, for lack of a better word, question number four probably hits the closest to that intersection.

Mary Jo Deering – ONC – Senior Policy Advisor

Deven, thank you. That was my point, too, that one way to distinguish, or one trigger, if I may borrow your own term, for where the potential catch point, the most obvious is, when it is an issue of authority, not so much the what, like what entities can provide them. Because that's the policy side of it and the Governance Workgroup said it would not set the policies to be executed but it would look at who should execute the policies that are recommended.

Paul Egerman – Software Entrepreneur

Those are great comments. One thing I want to say again about these questions is the way we're trying to structure today's call is we're going to provide you with some background information and then we're going to visit the questions again at the end of the presentation. So that when we visit at the end that would be the opportunity, if people think we should be asking one of these questions of this group that would be the point to ask them. I think it might be helpful to go through the whole presentation first. I also want to say besides coordinating with the Governance Group we also need to coordinate with the Information Exchange Workgroup, so I'm pleased that Micky was able to join us. But the Information Exchange Workgroup is doing a lot of work on something called provider directories, which will touch on a little bit about some of the things that we're doing here.

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

I have a question, Paul. The question was where you talk about the level of assurance, in posing that question are you referring specifically to the four levels that NIST and OMB have identified for e-authentication?

Paul Egerman – Software Entrepreneur

The answer to that is probably yes because that's what we're going to present to you in just a few minutes.

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

Oh, I didn't read ahead. I should have.

Paul Egerman – Software Entrepreneur

That's okay. The answer to that is probably yes, but as they say we're going to give you a chance to tell us if you think that's the right way to approach it. Again, as I said, we're going to revisit this. I don't mean to cut short questions about this, because people that are asking the questions are asking the exact right questions that we need to consider. But I also want to explain the background information that we're about to provide you, which is we're going to make sure that we touch upon the pertinent regulatory background information, the HIPAA security rule. We're going to review some of the recommendations that we already made, because we talked about coordinating with other groups, but we all ought to be coordinated with ourselves, so we want to make sure that we don't forget what we've already done.

NHIN exchange has already done something in this area, so we think understanding what they've done is useful. There's going to be a description of some generic provider authentication environments to make sure that we all are talking the same terms and language. Then exactly as you just asked, Dixie, we are going to go through the levels of assurance and do also some examples of what goes on with the federal e-authentication framework and NIST guidance. Then also the DEA, the DEA has done some things with controlled substances, and so we also want to make sure that everybody's on the same page to understand at least what has happened so far

So that's the background information. To start to dive into that, here is a slide on the HIPAA security rule. Are you able to go through this, Deven?

Deven McGraw – Center for Democracy & Technology – Director

Yes, I can jump right in. There's always a danger in putting just a snapshot of the security rule up and knowing that we've got a lot of expertise on the call on the security rule. But we're going to dive into the selected pieces of this that we thought were relevant, at least at a summary level. Then of course we have Adam on the phone, and Dixie, I know, knows a fair amount about this too.

So already the HIPAA security rule requires ... and now also the business associates to implement three types of safeguards in three general categories: administrative, physical and technical. This means that entities need to protect against any reasonably anticipated uses or disclosures of electronic protected health information, security rule only covers EPHI, that are not permitted or required under the privacy rules. Then they need to implement procedures to verify that a person or entity seeking access to electronic PHI is the one who is claimed, so the very habit that we are trying to get at here.

Now, it's important to understand not only what the security rule requires but also what it does not do, which is it does not mandate a specific implementation framework, nor does it specify authentication options or assurance levels or verification types. So I think this is important to lay that groundwork.

On the next slide with respect to what we've already said, we've already said—

Paul Egerman – Software Entrepreneur

Can people mute their phone? Somebody's typing real loudly.

Deven McGraw – Center for Democracy & Technology – Director

Yes, please mute if you're typing or doing anything other than listening. Thank you. All entities involved should follow fair information practices including implementing safeguards to prevent unauthorized or

inappropriate access, and we have already said that the provider has the responsibility for maintaining the privacy and security of a patient's record. However, they may delegate functions like issuing digital credentials or verifying identities as long as they do so in a trusted way. We also said that ONC has a role in establishing and enforcing clear requirements about the credentialing process. So it feels like we've opened the door for ourselves here with respect to some recommendations on that very point. The process must include a requirement to validate the identity of the organization or individual requesting a credential and here we've already made it very clear that we are engaging this topic at the organizational level. We also acknowledge that state governments might also provide some additional rules here as long as they meet the federal minimum requirements.

Does anybody have any questions about both what the security rule is or anything else to add on what the relevant provisions of the security rule to this particular topic, as well as some of what we have said in the past that is pertinent to the discussion we're having today? Okay, with that— We need to schedule more calls on Friday afternoon, I've got to say.

Paul Egerman – Software Entrepreneur

I know. Next, I think Arien should talk about NHIN exchange.

Arien Malec – RelayHealth – VP, Product Management

So for NHIN exchange there are essentially two levels under which authentication is managed. First of all, it's important to understand that NHIN exchange mechanisms, Nationwide Health Information Network exchange mechanisms, I should say, manage at a gateway to gateway level, where a gateway generally corresponds with what is known in the DURSA as a participant, and a participant is somewhat recursively defined as a signatory to the DURSA. But generally a participant corresponds to an organization or a super organization, so good examples of participants in the exchange would be clearly VA, DoD, CMS, and other federal agencies and federal partners, as well as large IDNs, and soon aggregators of other organizations such as regional health information organizations or state HIOs.

Mary Jo Deering – ONC – Senior Policy Advisor

Arien, I did just want to jump in and say that actually I think one of the newest signatories is at the level of a small provider, a small primary care provider practice.

Arien Malec – RelayHealth – VP, Product Management

Right, thank you for that clarification. So the definition of a participant doesn't assume that it be a large organization. I think the evidence to date has been that— The only implication that I wanted to draw out is that oftentimes the gateway and the associated participants may be a super organizational concept as well as an organization. Part of the infrastructure for exchange is an exchange certificate authority, and each gateway has a certificate issued by that exchange certificate authority, which has its self-defined mechanisms for ensuring the identity of the participants and the associated gateway. All transactions across exchange are gateway to gateway transactions and each transaction mutually assures the authentication of the two participants that are involved in that transaction, which is to say that there's both a high level of authentication and a high level of mutual authentication on each transaction that occurs in exchange.

The second level of authentication that happens on exchange is sub-participant authentication and participants are explicitly required to implement appropriate mechanisms and that the definition in the DURSA gives a definition of strong and appropriate authentication. It does not specify specific modalities or specific implementations of that level of authentication. Transactions across exchange may include information indicating that the participant has done that level of authentication, there's a technology called SAML, and assertions that can be assigned or applied at the transaction level that warrant essentially that the participant has performed that level of authentication.

But again, there's not a rigorous definition of what kinds of authentication mechanisms need to be performed by participants, and there's an agreed upon or built in level of understanding inside both the

DURSA and exchange that different participants may have different levels and different means of authentication, and that's actually one of the reasons why it's important in those transactions to carry what authentication was actually performed so that the receiving participant can decide in its local policy whether it approves or doesn't approve of that level of authentication.

So again, ... I think the approach for exchange actually validates at a high level the overall framing that Paul walked us through, that in exchange the level of authentication is done at the organizational level, at the machine to machine level, and that there is explicit recognition that sub-organization level or sub-participant level authentication needs to be performed according to the appropriate procedures that are performed by that participant for that purpose.

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

Who decides and at what level, who decides what an entity is? If you have a large integrated delivery network like Kaiser or Tenet Health, can the authentication be at the Tenet Health level, or is it each hospital or each clinic within Tenet? Is there a requirement at what level that has to be?

Arien Malec – RelayHealth – VP, Product Management

As I said, the definitions in the DURSA, so gateways tend to correspond – I'm going to back up. The authentication is done at the gateway level. There is no definition in the DURSA as to—

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

... where that is.

Arien Malec – RelayHealth – VP, Product Management

... and where that is. There is a definition in the DURSA about what a participant is, but as I said, it's recursively defined as a signatory to the DURSA. So there is no definition inside the DURSA or in the standards that constitute exchange about what level that gateway and what level that authentication needs to be performed at.

Paul Egerman – Software Entrepreneur

Arien, do you have any observations about how effective this is? Are people happy with it, unhappy with it? Is it working? Does it work?

Arien Malec – RelayHealth – VP, Product Management

Probably Mary Jo knows a lot better than I, I know that this process was arrived at with a long series of discussions about what could practically work. I believe that this processes approach was arrived at with a sense of reality, with a sense of understanding that there's a significant variety of local policies and procedures that are all sufficient to the purpose of achieving a high level of authentication for providers, and recognizes that it was infeasible, at least in the short term, to define a single nationwide standard that all participants could agree to. So that essentially the only workable mechanism was to hold it at the participant level, to hold authentication at the gateway level, and then require in the legal agreement the participants implement appropriate authentication and then again a third consequence, add the details by which they made the sub-participants, participant user authentication performed explicit in the transaction.

Paul Egerman – Software Entrepreneur

But is there a national standard at the participant level?

Arien Malec – RelayHealth – VP, Product Management

There is no national standard at the participant level.

Paul Egerman – Software Entrepreneur

But even at the participant level there isn't for digital credential?

Arien Malec – RelayHealth – VP, Product Management

Sorry, again at the gateway level there is a national standard, or rather, there is a national certificate authority, there's a certificate authority for exchange, and there is a uniform standard for supplying certificates for exchange.

Mary Jo Deering – ONC – Senior Policy Advisor

I think I would only caution against using the adjective “national” simply because of its implications when we're in rule making for governance. I think we are currently just trying to say this is a standard that is required for all those who participate in the exchange.

Arien Malec – RelayHealth – VP, Product Management

That's exactly right. There's a single exchange standard.

Mary Jo Deering – ONC – Senior Policy Advisor

Right.

Paul Egerman – Software Entrepreneur

Okay. I won't ask what the first “N” in NHIN stands for.

Arien Malec – RelayHealth – VP, Product Management

Nationwide, but not national.

Paul Egerman – Software Entrepreneur

Oh, I see. That's totally different.

Mary Jo Deering – ONC – Senior Policy Advisor

That's right.

Paul Egerman – Software Entrepreneur

Okay, so that's very interesting. Do people have questions for Arien? Do people understand what we're talking about so far or is everybody totally confused?

Deven McGraw – Center for Democracy & Technology – Director

I actually have a question. In distinguishing NHIN exchange from some of the other NHIN efforts that are being sponsored by ONC, I think it would be helpful to have some clarity about what it is. I'm mostly interested in what would motivate a small practice to sign the DURSA, to be part of NHIN exchange. Is it because they want an exchange with the current people who have signed the DURSA and are sharing data in accordance with those terms? Is it that simple?

Mary Jo Deering – ONC – Senior Policy Advisor

Arien, let me take a first stab at it. Yes, what you have said is true, that the federal agencies have determined that for them to meet their requirements for protecting their information that absent any other form of national governance that the stipulations in the DURSA are needed for them to feel comfortable and they're not willing to do it on a point to point basis. So, for example, as VA says, it really doesn't want to sign an individual, in fact, it refuses to sign 5,000 data sharing agreements across the country. So if you are an entity that does want to share with one of those federal agencies, then it's those agencies who have determined that this is what meets their expectations.

Gayle Harrell – Florida – Former State Legislator

Who actually holds the responsibility when there's a breach and how do you determine what is to happen to the individual entity that does have a breach or does not meet the level that it has agreed to meet on the DURSA? Who's the responsible party?

Mary Jo Deering – ONC – Senior Policy Advisor

I'm going to go see if I can find Mariann to answer that. My initial answer, while I go off to look for her, is that they have tried to push it down to the participant level. But I am going to go find Mariann, and I will come back.

Arien Malec – RelayHealth – VP, Product Management

The two pieces of information that I remember from my multiple readings of the DURSA—and again, Mariann is definitely the expert here—are that signatories of the DURSA ... have an explicit requirement to notify on breach and to remediate on breach. So part of the signatory process for the DURSA is that there is local autonomy and that there's local responsibility, but that there's reciprocal responsibility and that participants who notice breach of any kind have an affirmed responsibility to notify the participant.

Mary Jo Deering – ONC – Senior Policy Advisor

I found Mariann. The question on the table is responsibility in the case of a breach. Under the DURSA, who is responsible?

Arien Malec – RelayHealth – VP, Product Management

Hopefully Mariann says something identical to what I said.

Mary Jo Deering – ONC – Senior Policy Advisor

... you gave him the answer—

W

It's a test.

Mariann Yeager – NHIN – Policy and Governance Lead

Arien, I'm confident that it's going to be consistent. Essentially, the participants wanted to make sure that they had an obligation to notify each other if there was a dissected breach or a known breach that affected the transmission of data through the NHIN exchange and that had implications to other parties. So if it's within one hour where an issue becomes known and they have a reasonable belief that a breach occurred that has an impact to other participants or implications, the participants, they basically notify the coordinating committee and the legal points of contact for notice, a coordinated breach notification to those parties, they're put on notice that an issue may have occurred.

This is really important to the federal participants. In fact, it came up at the last minute after the DURSA had been cleared and ready for signature, and it was a show stopper that they absolutely insisted on it because it was something that they have to do for FISMA, and that the other party to the exchange felt that they could accommodate. Within 24 hours they're obligated to provide additional information regarding the nature of the breach and whatnot. The coordinating committee actually once they receive the one hour notification they have to convene themselves within 24 hours to determine if there's anything they need to do to take action, if they need to suspend termination, revoke their digital certificate or whatnot.

Deven McGraw – Center for Democracy & Technology – Director

I'll just add something, once the participating entities find out about that they have legal obligations under the stimulus legislation to notify individuals.

Mariann Yeager – NHIN – Policy and Governance Lead

Right, and this is absolutely complementing and in no way interferes or is intended to address their obligations under other breach notification rules. This was an additional obligation they felt they had to one another and to trusted exchange partners to know when there's been an issue that can have implications to them, because they frankly might want to make the decision to cut them off.

Gayle Harrell – Florida – Former State Legislator

That's my follow up question is who holds the stick and if there is an egregious breach that they feel the party, the entity is no longer a responsible agent, how do they get kicked out of the club? Who makes that decision and under what circumstances does that happen?

Mariann Yeager – NHIN – Policy and Governance Lead

There are several ways that can happen. One is that an entity, if they feel that they are creating a compromise there is some risk that other participants can take themselves off line, and that can happen within an hour, because simply the certificate is revoked and that happens, the coordinating committee, the exchange participants by signing the DURSA have given authority to the coordinating committee to make that determination. They also give the chair of the coordinating committee some discretionary authority that if there is such an egregious act, that they don't have to wait 24 hours to act, that he can pull the trigger, notify the committee, and address it that way. So it was a way to be responsive and to be able to take action as soon as an issue becomes known.

Paul Egerman – Software Entrepreneur

This is extremely helpful. I want to make sure that we keep our discussion focused on the issue of authentication. You're raising great issues, Gayle, because the hardest part of this whole thing is what happens if somebody doesn't play by the rules.

Gayle Harrell – Florida – Former State Legislator

Exactly.

Paul Egerman – Software Entrepreneur

What we're trying to do, though, first is define the rules, because you raise a good question. In response to the question was something that was very interesting and important that was said, which is that there's a vehicle to revoke the certificate. So the certificate really can be used as an interesting vehicle within this governance framework.

But to get back to NHIN exchange, if I'm hearing Arien correctly, the main components are—and we updated the slides while this discussion was going on—the main components is you have authentication at the gateway or machine level or what we're calling the entity or organizational level. That there's stuff that can happen behind the gateway, basically business processes and other things that might happen within each organization, and use the technology to communicate some information about what's called the SAML assertions about what's going on with user authentication.

The last bullet here is, again, I want to make sure I've got this right, Arien, it says, "Requirements for authentication defined at a high level of the DURSA not otherwise standardized," they're talking about the user authentication? There is a standard for the certificate that's being used by each of the participants, is that correct?

Arien Malec – RelayHealth – VP, Product Management

I think you got them all exactly right.

Paul Egerman – Software Entrepreneur

Okay, and an interesting model. So those are the questions for Arien on this. Are we ready to proceed?

W

Arien, who runs the certificate authority?

Arien Malec – RelayHealth – VP, Product Management

I'm actually going to turn that one over, I think, to Mary Jo or Mariann who know the details there.

Mary Jo Deering – ONC – Senior Policy Advisor

Mariann, did you come back online? I believe, again, that it is in the hands of the coordinating committee.

Arien Malec – RelayHealth – VP, Product Management

Yes, it's actually in transit right now. The contract for operations for the Nationwide Health Information Network is being reestablished. I believe it's under overall governance of the governing authority, which at this point is the coordinating committee with input from the technical committee for the ... of exchange. Over time this will migrate to the established governance process that will be established under the work that ONC is undertaking.

Paul Egerman – Software Entrepreneur

Interesting.

W

So each of the gateways goes there to get their certificates?

Arien Malec – RelayHealth – VP, Product Management

That's right. Part of the initiation and part of the on ramping or onboarding of a participant, there's a whole set of activities, including testing and conformance, that culminate, or at least one of the key culminating steps is in receiving the production certificates.

Mary Jo Deering – ONC – Senior Policy Advisor

I may have misspoken, and Arien, maybe you corrected me. ONC's technical team leads the onboarding process.

Arien Malec – RelayHealth – VP, Product Management

That's right. So ONC runs the onboarding process, it's done under the governance authority, which at this point is the coordinating committee, and will transition as ONC establishes governance.

Paul Egerman – Software Entrepreneur

Fascinating. So I think relevant to where we're going today is what is the scale that this was intended for or anticipated that can work as structured, and how does that compare to our target scale for our conclusions?

Arien Malec – RelayHealth – VP, Product Management

As always, that is a great question. I don't know the answer as to when the process was designed, what level of scale it was designed to. I know that right now the onboarding process is a rate limiter in terms of bringing up new participants. I also know that the teams that are doing onboarding are putting together some processes to make sure that they can accelerate the onboarding process, but I would also believe that because of the central model there is an inherent just architectural limitation in terms of the degree to which that model can scale. It was one of the architectural principles for exchange that it was a network of networks and that implied in that model is the concept of an NHIO, a National Health Information Organization, which, as Mary Jo rightly points out, not all the current ... are what you'd normally think of as national HIOs. But that's the architecture for which it was designed.

Mary Jo Deering – ONC – Senior Policy Advisor

That was where ... first stood up and actually he says the onboarding is a rate limiting factor. That's all totally in ONC's control. That's not a function of the exchange participants themselves. So that's as much a resource issue for us as many other things.

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

I'm going to disagree. I think that there's a fair amount of ability to turn up and turn down the resource, but when we're looking at the number of orders of magnitude, the difference between every practice in town and perhaps a few hundred networks that participate in a network of networks, it may not be simply a matter of adding more resource. It may take a different approach.

Mary Jo Deering – ONC – Senior Policy Advisor

Obviously this is all part of what should come out as a result of the governance process, is where does that responsibility lie?

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

I'm attempting to get at the issue of are we here discussing the process by which a network participates in a network of networks, or are we discussing something that is broader in its implication, which is how do each of 350,000 organizations authenticate with one another rather than through a hierarchy? I'll take guidance from the co-chairs on what we're talking about, but the issue that I've been driving about is not scale on a little bit or a little bit bigger, but substantial differences in scale here.

Paul Egerman – Software Entrepreneur

The answer, Wes, is when I started the call I thought it was the 350,000 entities, how do they communicate? But you raise a good question. So if it's okay with you what I'd like to do is proceed with the background information, and when we get to the five questions at the end I'd like to ask you to raise it again, because maybe we need to consider a hierarchical architectural aspect to this thing.

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

Paul, you're always trying to keep us on the agenda.

Paul Egerman – Software Entrepreneur

That's correct. But it's a great question. Are you okay with that?

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

That's fine.

Paul Egerman – Software Entrepreneur

Are there other questions about this and in exchange? Thank you, Arien, and Mary Jo. I guess Mariann's off the phone but it's really wonderful when people have questions and we can run out and get someone to answer them. So I really appreciate your help, and complicated issues.

Moving on in the agenda, we want to recap the definitions and then talk a bit more about the architecture. Was somebody at MITRE going to take us through this part?

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

This is Mindy Rudell from MITRE. I was going to take you through this part. So I'll get started, and if you have questions feel free to interrupt me and I'll be happy to stop and go over those. So just recapping the definitions quickly, the authentication part ... verification that a person or entity that's seeking access to something that's protected information is the person or the entity that's claimed. Then the level of assurance is the degree of the confidence that you have in that authentication attempt.

When you think about assurance and authentication, there's some notion that there's a range of options that are there based on the kinds of risk you're facing with the kind of thing you're trying to accomplish. There's also a notion that part of the answer for assurance and confidence is technology and process. There's also policies and governance, as we've been talking about throughout this phone call, that all contribute to that level of assurance or confidence.

The last definition on slide 10 is one that was not on the previous slide and that's the notion of a digital credential. So to talk about an example of that in certificates, the more general notion of a digital credential would be that it's the mechanism that's used to identify and authenticate the organization, it could be an individual, but in this case we're talking about organizations to each other. So why don't we go to the next slide, slide 11?

This is just a pictorial representation of a very simple version of an authentication environment. You can have multiple provider organizations, they could be of different sizes. Inside the organization they may have many different kinds of users, many different kinds of networks, many kinds of machines, but there's some notion that at a boundary there's something, some machine or some gateway that's representing the way that that organization is going to validate that it is the organization that it says to another organization.

So you can take any of these two provider organizations, and say they could be different sizes, they could have different networks within the organization, but at some point they want to validate that provider organizations is the one it states to another provider organization. The way they're going to go about doing that is exchanging some kind of a digital certificate. The little certificate pictures represent different digital certificates. They could be somewhat different from each other, as long as they all conform to some kind of a standard that allows them to use for authentication to another organization.

Paul Egerman – Software Entrepreneur

Before you go on, Mindy, I just want to point out that it says here provider organization, so that means it could be a hospital, it could be a medical group, it could be exactly as Wes suggested, it could be a solo practitioner. But it also could be a laboratory or a pharmacy in terms of stage one of meaningful use. It possibly could be a public health organization and I think also possibly a payer for an insurance company. One of the questions that we're going to be asking again is who can get these things in terms of what organizations?

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

Paul, that's a good point relative to your earlier scoping of our discussion, you said this was stage one meaningful use, which really only includes providers.

Paul Egerman – Software Entrepreneur

It includes providers but it includes laboratory transactions.

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

Right, I consider labs a provider.

Paul Egerman – Software Entrepreneur

Right.

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

But you just mentioned insurance companies and I don't consider those providers.

Paul Egerman – Software Entrepreneur

Yes, they're not, although stage one of meaningful use does have ... eligibility checks in it, right, so I think I could use that as an excuse to—

M

No, it doesn't, but we promised ... stage two.

M

....

Paul Egerman – Software Entrepreneur

So, I stand corrected on that issue. But anyway, the point is probably not a good one. My point was that we will have a question about who these provider organizations are as to what should be included and whether or not they're only provider, if that's what you're saying, Dixie.

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

Yes—

Paul Egerman – Software Entrepreneur

Because maybe there are some that aren't provider organizations, that have something like HIOs you probably want to have them and that will be an interesting discussion. Sorry I interrupted you, Mindy.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

That's no problem. A couple of other quick points. One is that the notion would be that the authentication would precede the actual information exchange, ... validate the organizations are who they say they are and then after that you say, okay, I'm satisfied that you are who you say you are and then the information exchange would proceed.

The other thing that this slide doesn't explicitly show is what we talked about earlier, the notion of onboarding, that somehow these credentials had to get to these organizations in the first place. So in some way they had to go out and prove who they are and receive some kind of digital credential, which then gets you, in the process afterwards, to validate and authenticate themselves to other organizations to enable information exchange.

If there's no questions on this slide any further, then I would move on to slide 12. Are there any other questions? Okay, so why don't we move to the next one?

Let's talk a little bit more about determining this appropriate level of assurance. In this case what we're going to do is look at an example from the federal government and it was referred to earlier as the authentication example. It's not that it's the only thing that could be used here, but we think it is representative of this notion of there being a range of different kinds of levels of assurance that are suitable to different levels of risk depending on the kinds of transactions we're trying to accomplish.

The federal government did find that the process they put in place, the lessons that were learned led them to this range of options which we think would inform the decisions that we need to make going forward. So we're going to talk a little bit about the ... in this e-authentication guidance, which has been focused on a range of things, including government to business and government to citizen interactions, and then also the DEA's e-Prescribing example, would HIT use this guidance to figure out what they were going to do going forward. So we're going to talk a little bit more about those.

With that, let's move on to the next slide. On slide 13, we're going to talk about ... e-authentication framework. There are several ideas that are useful to consider in this case. One is that this framework is an attempt to map risk to levels of security, so you can I'm trying to do something and it seems really low risk and so I'll use a mechanism that's suitable to that low level of risk. Or I'm going to try to do something that's pretty high risk and I'm going to take a mechanism that's suitable to that higher level of risk.

The whole framework was developed to meet increasing needs for the government to secure services that are expanding in all kinds of ways in terms of how the government interacts with businesses and the government interacts with citizens. The framework was put in place to really address a range of kinds of interactions that could happen, that do fit into different levels of assurance, different levels of risk. The e-authentication guide focuses on securing access to transactions over the Internet, and it's focused mostly on technology and processes. There are other aspects that you would need to deal with, like you talked about governance. It doesn't explicitly deal with governance issues, as an example.

Let's move on to the next slide, slide 14. This is a snapshot, on this slide, of the notion that there are increasing levels of assurance which are useful when you have increasing levels of risk for the kinds of bad things that can happen if something goes wrong. So this e-authentication framework includes a tool that you can use to select and appropriate level of assurance based on the impact that's due to something going wrong, some kind of authentication error.

The easiest way to think about this in my mind is that you can take the two extremes. Level one is pretty low risk. So if you think about it, when you use Facebook or Yahoo! E-mail, there's not that much—Facebook, let's take an example, in general the way it has been looked at early on, they weren't overly worried about someone getting access to someone else's Facebook account. They don't get a whole lot of measures to make sure that you really are who you say you are when you set up a Facebook account. You pretty much can set it up and then you can authenticate to it. There's not a lot of rigor behind that, which is perfectly fine for that kind of environment.

At the other extreme, you could have a data center operation sitting in the Department of Defense where they really want to know exactly who's coming in and have very high confidence that whoever tries to authenticate, or whatever organization would try to authenticate is exactly who it says it is. That's a higher level of risk and so there'd be a higher level of loss associated with something inappropriate happening. It's a—

Neil Calman – Institute for Family Health – President & Cofounder

Can I just stop and ask you a question for a second? When you talked about Facebook, there's actually no authentication if you go to set up an account, right? I could take a picture of my sister and set up an account in her name and pretend I'm her for the rest of time and she would never know it potentially or whatever. So to go back to your point about how you get the credential in the first place, there's actually no authentication when you go to set up an account. You can set up an account as somebody else.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

That's right, actually. You could easily pretend to be someone else, but there is ... authentication you would type in, but you could be pretending to be someone else and there'd never be a ... that says you really are who you claim to be. So that's exactly right, and that would be useful if you don't really care. If there's some services you want to provide in there, it's not that big a deal if you're doing that on behalf of your sister and it's not really her, it's really you.

Neil Calman – Institute for Family Health – President & Cofounder

I guess my point is just that as we're talking about these different levels, it seems to me like there's a bifurcation. Each of those levels has a level at which you're authenticating the person as it's getting set up, and then you're authenticating their reconections.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

I think that's right. I'm going to talk about that in just a second. That's an excellent point, and we're going to come back to that in just a moment. Are there any other questions?

There's a little example of a table in here, but I don't really want to go through that in detail. It's there for folks to look at, at their leisure. But the notion is that the potential impact for authentication errors as that increases you go to a higher level of assurance that's required. If there's no other questions let's go to the next slide, because I think it gets to your excellent question.

This table—and if you're looking at it online don't panic, I'm not going to go through all the boxes here. But the e-authentication concept includes several different requirement areas. So as we just were talking about, we could talk about the initial set up of an account or of a service as your registration process, what application process do you have to go through to obtain some kind of identity credentials. Now this, when you read it, seems very oriented towards individuals, but there's an analogy that would happen for organizations.

So an organization first registers. They have to go through some kind of process to get a credential. What that is varies based on the different levels of risk that are associated with what we're going to do going forward. So the examples here, I'll pick on this one, in level one you could do something remote, you could say whatever you want, kind of, is really what it comes down to. When you get to level two you

can be in person or remote; level three in this case in person or remote. When you get to level four you have to be in person, so there's a notion that the level of rigor goes up as you go to the upper levels.

They have other requirement areas as well, so just as you have to register there are also requirements for how do you prove your identity. In this case it talks about an applicant's identity. That could be an individual, but in your case of course you're talking more about an organization. There are requirements in the areas of naming, how you make sure there aren't naming conflicts, something that they call authentication token, which is really the technical mechanism that's being used to electronically prove the identity. There are record keeping requirements and there are requirements related to reusing some kind of existing credentials, with the idea being if you got a credential from some other organization could that be considered as a point of entry that you could re-use to get a credential in this particular environment as well.

I go through these just to point out that it's not just this specific of how you exchange a credential to authenticate, but there are other elements as well and in all those cases there's a notion of an increasing level of rigor to go along with an increasing level of risk. That concept, in our experience and also in the settled governance experience with the e-authentication framework, tends to apply in a large variety of cases where there's some kind of range in there, and this is an example of that. Are there any questions about this?

Neil Calman – Institute for Family Health – President & Cofounder

I'm thinking about certain systems that we're connected to and it seems like you can cross over between these levels. There's a system that could have a level four registration but only have level two as the point of reconnecting to the system.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

But usually they tend to go together. Usually it tends to be that if you want a certain level of confidence you're going to be going up and down that column in a sense for all those different aspects.

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

And if you don't it's a low water mark, not the high.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

Exactly.

Neil Calman – Institute for Family Health – President & Cofounder

For example, we have a very secure portal for our health department and to get an ID and to be able to log into this is a nightmare, but once you have it all you need to do is put in your password and you have access to it. There's no other authentication at the point of retrieval. It's kind of like you've gone through all of the hoops and loops to get—I guess I'm sort of confused. So at that point what you're saying is that system is only as good as its weakest link, which is putting in the password to get access.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

That's the philosophy behind this framework. Now in the case here we're talking about organizations, there aren't as many options. But when you do look at individuals, what's going on behind the scenes and what kind of credential you might issue to an organization, there might be some linkage behind the strength of what's happening within an organization and whether that influences the strength of assurance that you would grant to an organization as a whole. But in this case it is the weakest link. I think that's a fair statement. It's looking at the low water mark.

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

However, we should point out that within a single organization you could have a level four, for example, authentication could be required for getting psychiatric notes or something, right, whereas, a level two

might be required to log into your desktop or something? You have policy that's application and situation specific.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

Thank you, Dixie, because that's exactly right, the notes that you want arranged, because it gives you the flexibility to accommodate the level of risk with which you're dealing, is exactly what you want. You want to find a suitable level for what you're trying to accomplish.

Neil Calman – Institute for Family Health – President & Cofounder

Right, which incidentally coincides a lot with the way an exchange handles things, where the organization can decide what to do within the organization—

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

Yes.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

Okay, so let's go to the next slide and look at the example from DEA. Here was DEA and they tried to use this e-authentication framework. The DEA rules for electronic prescriptions of controlled substances, they were trying to move toward electronic in place of paper or other processes and so they looked at these rules and said how can we apply them. The initial risk assessment that they did led them to a selection of a level four assurance. They had several areas of high impact that drove them up to looking at it in terms of what the authentication errors could mean to them and that led them to a level four. But they had resistance from some set of stakeholders because the requirements seemed too stringent and they just seemed too out of the ordinary for the environment in which they were dealing. So they paid a lot of attention to analyzing those burdens that would be put in place here.

So the path the DEA took was to introduce mitigating factors, things that they could do to lower that risk and then lower the selection of the level down to level three. So they did things like they put in place mechanisms that did a better job of separation of duties that were going to really look at who can do what, and by separating duties we're going to reduce the level of risk in our overall environment. They had system access controls. They looked at how to certify implementations, and that set of activities, those mitigating factors, let them make the case to go down to level three. That allowed them to ... what they do and ... a lot of agreement, a more classical implementation for their environment.

So they tailored the use of this framework to exclude options they viewed as unacceptable and to find a path that would be practical but still meet their needs. I think that that notion that you can look at this as a framework, guidance and then figure out how to tailor it to your environment is a good one. It's not a one size fits all. There are ways to ratchet things up or down using additional mechanisms, additional thoughts about how to communicate the risk and allow you to take an approach that seems practical for your environment.

Let's look at the general experience with e-authentication, that framework, and slide 17. The idea here is if you look at the industry experience overall—

Paul Egerman – Software Entrepreneur

Can I just interrupt you a second, Mindy?

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

Sure.

Paul Egerman – Software Entrepreneur

Can you just go back to the DEA experience, it does relate a little bit to your next slide. But I'm curious, is John Travis on the call?

John Travis – Cerner – Sen. Dir. & Solution Strategist – Regulatory Compliance

Yes, I am, Paul.

Paul Egerman – Software Entrepreneur

I'm just kind of curious, John, you're stepping in for— David McCallie couldn't make it so you're with Cerner, but I understand you have some experience with how DEA turned out. Do you want to tell us anything about—?

John Travis – Cerner – Sen. Dir. & Solution Strategist – Regulatory Compliance

I've got a couple of experiences. One that is close to the DEA, and that's with Ohio, which is probably the one state in the union that required something pretty close to the DEA model for e-Prescribing, where they do use advanced authentication that in our experience certainly is very comparable. It's informing a lot of the work we're doing with DEA. In Ohio, they require use of advanced authentication for the full range of medication management events, whether in an ambulatory or an inpatient environment, so order verification, administration to stenting. We have encountered both use of advanced authentication methods within the four walls that were based on biometric approaches that are very similar in the reliability levels that the DEA required for their biometric option, and this is for personal authentication. Then outside the four walls using more of the hard token approach, using a FOB that generates a random number and you access a FOB or use it with a PIN.

The thing that we really found that made that experience seem to work is the more you can leverage single sign-on for methods that were already in use for user authentication, so the doctor is using the same advanced authentication method to do initial authentication to the system and for doing electronic signature for carrying out that order verification, and something of that nature really needs to make it work. If you're asking the physician to carry around multiple, distinct authentication credentials for different purposes, now you're going to find resistance to adoption, they could lose one of them, you're making it difficult. It's not what's provided through their institution.

Now, the DEA predicates at least some of their approaches to involve the hospital and its medical staff function to serve in the registration authority role and may deem certificate authorities similar to what have been discussed, but that seems to be the big lesson, you've got to find a method and an approach that can be leveraged for more than just the purpose at hand. The DEA certainly allows for that as long as the security credential can be conveyed or embedded in a method specific for the use for controlled substance e-Prescribing. I don't know if there's more that we can say, but I think that that's the practical matter is that the more it can leverage something that's already in use the chance for adoption success is going to be greatly improved.

Paul Egerman – Software Entrepreneur

Has there been a lot of adoption success with the DEA thing?

John Travis – Cerner – Sen. Dir. & Solution Strategist – Regulatory Compliance

Again, with Ohio; with the DEA not yet. The practical matter is the thing that's standing in the way right now is enabling the transacting of the controlled substance e-Prescription through the intermediaries, particularly through SureScripts, because they've got work that is scheduled to be completed and I would imagine shortly after the first of the year you'll see some real use begin to come into play. But that still stands in the way, and not in a negative way. That's work they needed to do. Ohio still stands, if you go look at real uses in Ohio it's going to come pretty close to what the DEA's doing, with some exception as to the workflow itself in the clinical application because the DEA rule calls for controlled substances to be fairly well segregated out and other things the position might be signing, it involves additional work steps to mark things as ready for signature. But it certainly is very close in the methods that are used that the DEA would also find supportable.

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

Does the DEA prescribe any requirements for how the authentication is implemented in the system, like whether the application can do this two factor authentication, or whether the application has to use operating system services to do that?

John Travis – Cerner – Sen. Dir. & Solution Strategist – Regulatory Compliance

It does. There are a couple of paths. The DEA rule lays out a path that if there's a personal digital signature used you don't have to have server or machine level certificates used, because there's a data set that's a subset of required information for the controlled substance prescription that has to be digitally signed in the end for record keeping purposes, both by the prescriber and by the receiving pharmacy. If the prescriber uses a personal digital signature, that addresses the requirement. If they don't, then the last intermediary between the prescriber and the pharmacy or the pharmacy itself must use a machine certificate to sign the controlled substance data set in order for that record keeping to be seen as being of integrity and hold validity for audit purposes and record keeping purposes.

If you don't use that personal signing method, then that pushes the burden for that digital signature basically downstream, if you will. Then there also are specific workflow steps such as the controlled substance prescriptions have to be marked for approval to be signed, it can be done by the physician or it can be done by somebody that acts to help prepare that but they can't sign it. Only a licensed independent practitioner can sign the prescriptions for controlled substances. They have to be segregated from non-controlled substances as to the signing action and you have to sign within a patient context. You can't queue up controlled substances to sign across patients and have the prescriber sign across all patients in one action. They could sign multiple controlled substances for a patient at one time.

Paul Egerman – Software Entrepreneur

Fascinating. That's very helpful, John. I'm sorry, Mindy. I hope I didn't take you off track.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

Oh, no problem at all. Let's move on to slide 17. Just quickly, if we look at the experience with the e-authentication framework we somewhat argue, but I don't think much, basically we have a lot of examples for low assurance huge populations widely implemented over the Internet, various approaches there. There's a lot of good examples for high assurance with much smaller populations. The thing that's been difficult so far is to find proven technical approaches from moderate to high assurance for very large populations. When you look at that mix of the size of a population and the scale that you have to deal with, as well as the level of assurance, it's a little bit more of a challenge as you get larger and larger and you're looking for moderate to high assurance. So that's an area to keep in mind as you go forward in terms of what to look out for and what to keep in mind as you look for solutions to deal with that part of the range of risk and population size.

On slide 18, there's an example that comes from the online banking industry, and it's just a couple of quick lessons learned. There are also example policy statements, which for the folks who have the slides you can look at at your leisure as a way of how another industry looked at putting policy forward in this area. But the main points that I think are worth discussing here is if you look at the policies that they issued for online banking, in August of 2001 they had to change some fundamental concepts and reissue the policy by October of 2005.

So the takeaway from that is you really need some agility in your policies that it might be that the situation on the ground changes in some way that says, you know, I need to change things. That's what they said around here and an example is they had a policy statement that the method of authentication should be appropriate and commercially reasonable and they talked about specific things like single factor authentication is widely accepted. By October 2005 it was no longer that way. They basically said it was not adequate and needed to change the language, which ... the situation then. That kind of flexibility is something you can bake in. You can say, you know, here's an area where it might be necessary to change things downstream and just have that as something in your thought process as you proceed.

The other thing that was interesting in looking at this online banking industry is that they added in some statements because they found they needed to monitor the effectiveness and adjust the policy as they went forward. So that notion that you might need to look at monitoring the effectiveness of the policy and the methods that we put into place is another thing to keep in mind, another lesson learned from looking at online banking for thinking about for the health care environment.

With that I'd like to summarize some of the considerations that we talked about and how they can apply. It's slide 19 that we're going to move to now. The e-authentication framework that we talked about was developed primarily for individuals when you look at the language, not organizations, although it's certainly being used now and they tried to adjust the language so that it does ... organizations as well. So you can look at government to business and you're talking organizational there, but some of the language does look like it's more for individuals. A lot of the concepts still apply.

The framework's also more focused on technology. It's not really dealing with governance and policies per se. But the framework has a lot of information that is useful to consider. The framework can easily be tailored for use in any kind of environment, including health information exchange, but there's some practical consideration of implementation that may not be fully addressed. So if you look at the kinds of risks associated with the kinds of things you're trying to do, it takes you to a higher level of assurance that's needed and you still have a fairly large scale at some point. So you have to figure out what kind of flexibility do you need, when do you need multiple solutions and not just one, and take those into account as you go forward. The framework does not fully address that. It partially addresses it.

Any adaptations that you have really does need to reflect this range of risk assurance and types of transactions. It was one of the strengths of this framework, that it took that combination and said we're not just going to look for guidance and say one solution fits everybody, but instead say that there are really different kinds of approaches that are suitable to different kinds of environments and that even within one environment I might look at different kinds of solutions depending on the risk associated with the type of transaction I'm looking at accomplishing. There's some experience from other industries that could be beneficial. We were talking about the NHIN exchange and we were talking a little bit about, SAML came up, SAML, and there are other identity federation technologies, how you pass on information from one organization to another that's useful in terms of deciding the level of trust for going forward and doing additional things. So there are some other things going on in terms of the trends that we're seeing in industry that are beneficial to look at to inform the policy that you come up with.

Lastly, when you think ahead and think about the auditing element and the kinds of authorizations that you might need to check before completing an activity, especially if you move on beyond the initial phase, it might be beneficial to consider attaching the notion of the requesting party's credentials and the organization's credentials to a request for exchange, so when do you need to know who kicked off this request, not just the organization that's at each end of the pipeline. So that's something else to consider as you look forward.

With that, I think we're back to the key questions for the Tiger Team and I'll stop talking.

Paul Egerman – Software Entrepreneur

Before we let you stop talking, Mindy, let me first say thank you very much. That was excellent, very helpful. Do you people have any questions for her?

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

I have one question for her, Paul. That is, she said that the OMB in this framework doesn't allow flexibility, and it really doesn't have any specifics on it. In what way doesn't it allow flexibility in implementation?

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

The thought there was that if you look at some of the rules in place, especially the higher levels of assurance, there's kind of an implication of a certain kind of technology, that you have to go in person for identify proofing, there are certain rules that seem to take you toward certain technologies and not other technologies. So in that way I thought that there was a little bit less flexibility than there are in some other cases, and that that might be worth looking at other industries that have wide presence on the Internet and see if there's anything from there that might inform the path that you want to go forward depending on the scale at which you're viewing.

Arien Malec – RelayHealth – VP, Product Management

I think one good example of that when I was looking at this particular area was there are specific requirements, for example, examination of financial databases and financial records, that make perfect sense for general purpose authentication in individuals. In a clinical context, you can actually get to an equivalent level of assurance by examining, for example, licensure, checking licensure against databases and those kinds of things.

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

Oh, sure—

Arien Malec – RelayHealth – VP, Product Management

It's not clear the ... level give the level of flexibility to get to the same outcome with different input.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

Just one other thought along those same lines, this guidance specifically excludes something called knowledge base authentication, which is kind of a term of ours seen dancing around on some of the Internet authentication providers, and that notion of knowledge based authentication is exactly what you're saying. Look at information you have and use that as part of the decision making process. That full concept is not explicitly addressed at all in the—

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

I see. I thought you were saying it was dictating a particular technology. I see what you're saying.

Paul Egerman – Software Entrepreneur

Any other questions for Mindy? Thanks, again, Mindy; excellent presentation, very helpful. What you see on the screen is the five questions again and I'd also remind everybody that we are looking at stage one meaningful use exchange transactions but not 100% limited there. We'd like to make sure we do something that is useful thinking ahead to what might occur in future stages. The issue here is I'm going to review very quickly these five questions again, but the fundamental question I want to ask you is, are these the right questions? In other words, do we want to change things? Do we want to add anything? Then at the next meeting hopefully we will begin answering them.

So the first question is the strength of provider entity authentication, in other words, the level of assurance. In other words, trying to decide what we want for this provider entity authentication. Again, a reminder, we're not talking about authenticating individual users, we're talking about entities or organizations. The second issue is which provider entities can receive digital credentials and what are the requirements to receive those credentials. That's a question that's probably related to the discussion that Dixie and I started to have when we looked at the diagrams and who are the people who really get these digital credentials.

The third one is what is the process for issuing digital credentials, including evaluating whether initial conditions are met and reevaluating on a periodic basis. In some sense part of the answer to that relates to some of the comments that Neil made about a system where he said you have to go through some hoops and process it, so the question is what is the process going to be. There's a fourth issue, is who has the authority to issue the credentials. The fifth issue is a standardization certification question, is should we raise this to the level of certification.

My question to the team is, are these the right questions? Do the questions make any sense? Should we fix them? Should we change them? What do you think?

Gayle Harrell – Florida – Former State Legislator

I had one question on the first question. In your comments you're talking only about authentication of entities, not individuals. Whereas, in the previous discussion that we were having ... examples, there were individuals talking about being part of NHIN. So are you saying that we're only going to look at entities that have other members to them? If that's the case, what standard of those other members are they going to be holding the other members to ...?

Paul Egerman – Software Entrepreneur

What do you mean when you say "other members?"

Gayle Harrell – Florida – Former State Legislator

For instance, if we're talking about an organization—say, a large hospital system—and they're the entity that you're talking about and they get the digital credential, they have the authenticated entity. Then you have other people who are going to be part of that, individual physician offices, individual workers, whatever. Is that entity that is authenticated then responsible for authenticating the people below them?

Paul Egerman – Software Entrepreneur

I guess my answer to that would be yes, especially since the way you think about these things and we talk about entity organizations, but as you think about directed exchange and stage one meaningful use you've got really one EHR system or one computerized medical records system communicating with another computerized medical record system or another computer system probably. It may not necessarily be a medical record system but another computer system in the case of, say, a laboratory, but because of that the authentication at that sort of organizational level and that organization responsible for what happens behind that or within its four walls, or they have more than four walls, I suppose. But that would be my answer, unless people want to give a different answer.

Deven McGraw – Center for Democracy & Technology – Director

Paul, I think that's right. Recall that at the very beginning we made the assumption that organizations would of course have to have processes and policies in place to appropriately identify and authenticate the individual users within their organizations. I think that when we addressed the entity question if we thought there were some policy guardrails or guidelines beyond what's already in the security rule that we wanted to lay down for organizations to meet with respect to individuals I think we could get to that point. But we're trying to solve for the computer talking to computer issues first.

Gayle Harrell – Florida – Former State Legislator

Okay. Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Question number four, I'm wondering if—and I don't even know the answer to my own question but I'm throwing it out there. Maybe the question isn't so much who has the authority to issue digital credentials, but whether there are certain policy requirements that an entity issuing credentials would need to meet. I'm trying to think of a way to skirt past some potential Governance Workgroup issues, some of that overlap, where they're trying to solve for the who versus the what.

Paul Egerman – Software Entrepreneur

So your suggestion is to change it for, instead of who has the authority, is what are the requirements for organizations that have the authority to issue credentials?

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Software Entrepreneur

So instead of saying who we're saying in effect what's the application process—

Deven McGraw – Center for Democracy & Technology – Director

Well—

Paul Egerman – Software Entrepreneur

What's the skill, what do you have to do to be able to do this?

Deven McGraw – Center for Democracy & Technology – Director

Right. I don't know if it's what are the skill levels or what are the characteristics—

Paul Egerman – Software Entrepreneur

“Characteristics” is a better word, yes.

Deven McGraw – Center for Democracy & Technology – Director

... yes, of digital credentialing authorities? It's just a suggestion and we may just want to have an off line conversation with the governance folks to make sure that we're ... in a consistent way.

Neil Calman – Institute for Family Health – President & Cofounder

I have a question. I had to step away for a couple of minutes so I apologize if somebody discussed this, but when you're talking about the organizations there are all types of organizations. Our institution is a state licensed provider from the point of view of health care, but there's group practices that are just conglomerations of doctors working in one place that might share an EHR, like if we're going to talk about a designated entity that has some authority, those entities could have all different types of structures, some of which might actually carry with them a level of legal responsibility and some of which might not. Do you know what I'm talking about?

Paul Egerman – Software Entrepreneur

Absolutely. But isn't what you're talking about question number two that we have to decide, which entities get these digital credentials?

Neil Calman – Institute for Family Health – President & Cofounder

No, not really. When you say which entities, maybe I misinterpreted the “which,” but I was thinking more like are there characteristics of those entities in terms of just in general how they need to be licensed themselves or organized within a state in terms of responsibility. But maybe that is two.

Paul Egerman – Software Entrepreneur

Yes, maybe we didn't phrase it right. It says, “Which entities can receive digital credentials and what are the requirements to receive those?” So—

Neil Calman – Institute for Family Health – President & Cofounder

That could be like what type of corporation do you need to be?

Paul Egerman – Software Entrepreneur

Yes. One answer you could give, like if you put out a straw man answer it's probably not going to be a good enough answer, you'd say that well, you have to be licensed in the state. Maybe that doesn't work in every state for some reason, but that could be an answer.

Neil Calman – Institute for Family Health – President & Cofounder

Just incorporated but actually licensed as a health care entity?

Paul Egerman – Software Entrepreneur

Yes, that could be one way to answer the question.

Neil Calman – Institute for Family Health – President & Cofounder

I see.

Paul Egerman – Software Entrepreneur

So that's what the question is intended to ask, I think. Does it fulfill that in your mind?

Neil Calman – Institute for Family Health – President & Cofounder

Yes. I don't know the legal background of the different types of organizations like an LLC or a group practice or whatever. Some of them have real legal standing within, like if you practice in New York it has no legal standing, it's just a conglomerate, but they might be huge. So I guess I was thinking more in terms of what are the legal requirements? Do they need to be able to have some legal authority within the state to do something like this? We don't need to belabor it.

M

Paul and Deven, as a rule I think wherever uses the word "who" in these questions as opposed to "what are the characteristics and attributes of something like that," we're sort of going to be on a continual sliding scale of how specific and what are the defining characteristics for who that we're dealing with.

Paul Egerman – Software Entrepreneur

That's a helpful comment. You're right. That's the real issue is what are the characteristics and attributes, what was the other thing you said was?

Deven McGraw – Center for Democracy & Technology – Director

Characteristics and attributes.

Paul Egerman – Software Entrepreneur

Yes. That's really what we should be asking. That's the way to respond to Neil on question two and also, Deven, on question four, right?

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Software Entrepreneur

That's really what we're asking, for the characteristics and attributes. That's very helpful.

M

That's why the professor can say it better, you know?

Paul Egerman – Software Entrepreneur

That's very helpful. Wes, you also had a question, we were talking earlier about hierarchical versus just directed exchange and I sort of put you off on that question. Did you want to raise that issue again or are you okay?

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

I don't know that it necessarily shows up in the phrasing of these questions. I just am concerned that we are including scalability. I think you made the comment that you started the call saying that this was for the 300,000 practices level and I think that's fine with me for now, as long as we end up not assuming, making any other implicit or not even assuming but not thinking about issues of scalability downstream.

Paul Egerman – Software Entrepreneur

It's interesting, 300,000, once that seemed like a big number, but in the scope of some of the things that Mindy was talking about it's actually a small population.

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

She called the Department of Defense a small population.

Mindy Rudell – MITRE Corporation – Chief INFOSEC Engineer

I hope nobody tells them—

M

I think when we get to the point where we have enough device addresses to address every atom in the universe separately, that would be a large population. But I think the real issues, when I'm thinking of mentioning scale, I'm mentioning whether we think there needs to be levels of delegation involved in this process or not. I don't know. It would be interesting to look to see how retail establishments get on boarded for the credit card agencies, whether there's any delegation involved there or whether it's one giant entity that does it all, and if so how big is the entity.

Paul Egerman – Software Entrepreneur

That's interesting. Does anybody have the answer to that?

Deven McGraw – Center for Democracy & Technology – Director

It's a very interesting question.

W

I think each bank authenticates the different merchants, whoever has your bank account.

Paul Egerman – Software Entrepreneur

Yes, in general I think it is delegated, except for American Express, right, because they're not a bank.

Leslie Francis – NCVHS – Co-Chair

I think there's actually a pretty complicated set of legal standards that apply to the financial side of things. As far as I know the health side has never really looked carefully at whether they're a good model, and I think it would be terrific to do that.

M

Yes, I think that this also indirectly relates to the other topic that Mindy brought up, which is validation by what we know. We're dealing with authentication in both the sense of—and I've always had trouble with the term because of it, but I normally hear the word authentication being applied to the online interaction that confirms a pre-established identity. But we're also using it here for establishing that identity, or I guess a six step process that includes both of those two steps. Certainly in the case of a bank doing a credit card, they have already legally been required to authenticate someone just to have an account, so they're able to refer to what they know to add on credit card processing. I guess I'm just wandering here. But I think we understand our challenge.

Paul Egerman – Software Entrepreneur

Right. On the issue of the analogy to the banking and the comment that somebody made about banks able to delegate, I do want to point out what was said a little bit earlier in the presentation, that we already made a recommendation that says the providers can delegate this responsibility if they want to, in terms of issuing certificates. So that's just an observation.

Deven McGraw – Center for Democracy & Technology – Director

Yes, we did. So we are definitely onboard with that concept, but the stuff that we didn't get to that I think we need to in the next set of conversations is well, how will trust be maintained if that gets delegated, like what are the characteristics and attributes?

Paul Egerman – Software Entrepreneur

Well, that's true, although you could picture it as part of answering these questions. Similar to the analogy with the retail organization and the bank that Gayle mentioned, you could have a small group practice and maybe the physicians have, I don't know, admitting privileges at a local large hospital and they asked the hospital to take care of getting them their certificate so they don't have to hassle with it.

Deven McGraw – Center for Democracy & Technology – Director

I think that makes sense.

Paul Egerman – Software Entrepreneur

Yes, especially since it's also consistent with, you've got the ... exception and everything in terms of different relationships. Getting back to these questions, are people comfortable with this? I feel like this is like, what was the program, *Mission Impossible*, our mission, should we decide to accept it, would be to answer these five questions. Are we willing to accept answering these five questions?

Gayle Harrell – Florida – Former State Legislator

I think that probably the first five— There probably are more that will come up as we go into those five.

Paul Egerman – Software Entrepreneur

Right.

M

We need to know whether the secretary will disavow us if we—

Paul Egerman – Software Entrepreneur

Probably will either way. It's hard to know. I think Secretary Sebelius will never disavow us no matter what, complete confidence in our secretary. So let me take a peek going forward in terms of the schedule. We have another meeting on November 8th and the idea was to continue this discussion on provider entity authentication. Something that I don't know if we sent out, I don't know if we sent out the announcement yet—

Deven McGraw – Center for Democracy & Technology – Director

No, we haven't.

Paul Egerman – Software Entrepreneur

... everyone should hold the date, December 9th we want to do a hearing on patient matching systems. The direction that we're trying to head to, just to get everyone on the same page, is we're trying to do this provider entity authentication piece so then we're going to move from there into issues relating to patient access and patient matching. The intention is to say, well, we're in the area of interesting discussions about authentication and trust and so first we'll do it at an organizational level but then we'll do some of the same stuff at a patient level. What we'd ideally like to do is spend the rest of October and November and December doing provider authentication and then patient matching and patient access, because that would be a great accomplishment if we could get through some policy guidelines in those areas. I don't know if anybody has any comments on that.

Great. So as I said mission impossible, it sounds like we've got—and perhaps it's a mistake for me to phrase it that way, I'd just better phrase it as this is a challenging issue. This is a very exciting and challenging issue. We have an opportunity, I think, to make a good contribution to something that's very important.

Deven McGraw – Center for Democracy & Technology – Director

Call it Mission Possible.

Paul Egerman – Software Entrepreneur

Mission Possible, even the TV programs were a piece of cake, right? So this is Mission Possible and Mission Exciting, so this is a very good thing to be doing. What we're going to ask you to do—we'll give you a little bit of homework—is first, I want to remind everybody to review the transparency document that we're about to make that final, so if you have any last minute changes you want to make to that, if you could get that to us by noon on Monday. But then we're going to ask you to start thinking about these five questions, and I would especially appreciate if people have any guidance as to how best to approach these questions.

Should we just ask MITRE to list each question and put through some sample answers? What's the best way to approach this so that we can walk ourselves through this in an efficient way? Deven, do you have any reaction to that?

Deven McGraw – Center for Democracy & Technology – Director

I think we could also ask the Tiger Team to scope out how—if they've given some thought to this—how they would answer these questions.

Paul Egerman – Software Entrepreneur

That's great. So we'll send it out in the form of an e-mail or something.

Neil Calman – Institute for Family Health – President & Cofounder

I'm sorry, I'm confused. But it sounded to me like we were presented a model that has different levels of authentication, but it doesn't sound like from this question we're sort of assuming there's one solution, right? These five questions talk about a single system and one of the questions that's missing in my mind, and maybe I'm misunderstanding this, is what types of transactions that we're considering consider what levels of authentication? I don't know whether that's something that's within scope. Do you understand what I'm saying?

Paul Egerman – Software Entrepreneur

Yes, and so let me answer your question. The types of transactions are, first what was in stage one and meaningful use.

Neil Calman – Institute for Family Health – President & Cofounder

But most of that is really push stuff, right?

Paul Egerman – Software Entrepreneur

That's correct.

Neil Calman – Institute for Family Health – President & Cofounder

So it doesn't even require a lot of what we're talking about. It requires more addressing than people trying to come in and get information that they're not justified in getting. It requires in the first stage some registration process but not so much of the authentication at the point that they're going to be asking for information, because we're not really doing that in stage one.

Paul Egerman – Software Entrepreneur

Actually, I think all of these steps are needed for push.

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

Yes, they're needed in order to establish the two-way trusted path between the two entities, where the two machines are required in the standards, even in stage one, to mutually authenticate themselves. That's a requirement. These are what level of authentication is needed in that mutual authentication step.

Neil Calman – Institute for Family Health – President & Cofounder

Okay, go ahead, Paul.

Paul Egerman – Software Entrepreneur

You said go ahead—

Neil Calman – Institute for Family Health – President & Cofounder

In terms of different levels of authentication are we going to be talking about what types of transactions require different—

Paul Egerman – Software Entrepreneur

The starting point is, as I said, what you call the push transactions in stage one of meaningful use, so that's like the patient summary. It's test results. It's communication with public health organizations. Those are the key things. I think there must have been claim forms and payment stuff I hope.

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

No, it was taken out, remember?

Paul Egerman – Software Entrepreneur

I forget what was taken out. Those are the key ones to get started with. You ask a good question about what's going to happen going forward and so we should keep that in the back of our mind. We want to design something that can be used for what we think will go forward. We just have to be careful that we're not speculating on something that we don't know how it's going to work.

Neil Calman – Institute for Family Health – President & Cofounder

Well I guess my point is it seems to me like some of the things we're going to be doing going forward are going to require the highest levels of authentication, but that stuff you just mentioned doesn't in my mind of course. So therefore I'm not clear on how we answer these questions if we're really thinking about things at different levels.

Deven McGraw – Center for Democracy & Technology – Director

But to me, Neil, you would answer that question with saying if it's only a push transaction I would put it at a different level. That's part of answering the question.

Neil Calman – Institute for Family Health – President & Cofounder

Right. I'm sorry, because I'm so inarticulate it's like I'm speaking a foreign language, but from that point of view then, that whole process might be different, right? So somebody might be able to get the authority to do certain of these transactions in a different way that they would get an authority to do, like a level four transaction. Are we contemplating that people would have different types of authority granted in different ways, or are we going to go for the highest and best? Right now we want everybody to get this kind of certificate so that it's robust through all of the future developments that we're going to do.

Paul Egerman – Software Entrepreneur

My response to that, Neil, is that's the answer to the question. In other words, if you think we should do a tiered approach, do something for stage one and then something different for the others if we need to, that would be one way to answer the question. Another way to answer the question would be to start at the highest level, assuming that that's what's going to be needed eventually. What I'm saying is I don't know the answer to your question. In some sense by asking the question you're putting forward a great consideration that we have to—

Neil Calman – Institute for Family Health – President & Cofounder

Yes, I would make that question six in my mind, because it sort of wraps the things in terms of what we would do right now, in my mind.

M

Could you restate then what you say question six is again?

Neil Calman – Institute for Family Health – President & Cofounder

It's what types of transactions do we contemplate? We know stage one but we don't know stages two and three yet. What types of transactions do we contemplate and are we looking at a single level of authentication that would cover all of the future potential uses of information exchange or are we looking at different levels of authentication for different types of processes? If so, of course from my side I'm thinking of what does that mean in terms of the provider burden that you're doing different types of things at different levels? I think that's why that's important, because I keep going back to that framework that was shown.

Paul Egerman – Software Entrepreneur

Okay, we will add that as a question. I appreciate that, Neil. So starting to wrap up, because it's Friday afternoon and we also want to make sure any members of the public have an opportunity to say something, so what I'm going to be asking people to do is, again, is by noon at Monday respond if you have any last comments on the transparency document. We'll send out an e-mail with the now six questions. We want you to begin thinking about it and begin framing what you think is the way that we should respond to those questions so that when we get together on November 8th we can dive in.

Let me thank everybody for their enthusiastic participation on a Friday afternoon. I understand this was a short week and everyone was so busy they probably forgot it was a short week.

M

Some people had a short week.

Paul Egerman – Software Entrepreneur

Some people had a short week, some people did not. Thank everybody and if there are members of the public who would like to make a comment, Judy, can you open the lines to the public?

Judy Sparrow – Office of the National Coordinator – Executive Director

Operator, would you invite the public if they wish to make a comment to identify themselves, please.

Operator

Caller, you're in queue. Please identify yourself.

Carol Bickford – New York Nurses Association

My name is Carol Bickford from the New York Nurses Association. As you were moving through the presentation on slides 12 and 13 you identified government to business and government to citizen interactions as needing new authentication capacity. My question is, why do you not address government to government and citizen to citizen communications as those become part of our infrastructure for the Nationwide Health Information Network? Has that conversation been identified as not being germane or has it not been part of the conversation, particularly in light of the hackers and so on that have become our most common enemies in relation to our government to government actions?

Paul Egerman – Software Entrepreneur

I think what was on slide 13 related to the e-authentication framework as opposed to necessarily what we're going to be doing. But I think you're raising a good point and I appreciate the comment.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you, Carol. Are there any other comments?

Operator

We do not have any other comments from the public.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you.

Paul Egerman – Software Entrepreneur

Terrific. Let me again thank you, Carol, for calling in. I appreciate any members of the public who may have been listening to our call. We will start putting some information on the SACA blog that the HIT policy committee has, because we would like to see if we could solicit more public comment. I want to thank everybody. I especially want to thank the people from MITRE and Mindy who put together the presentation, and Judy Sparrow and the members of the team. So have a good weekend. Thank you very much.

Deven McGraw – Center for Democracy & Technology – Director

Thank you, Paul.

Public Comment Received During the Meeting

1. Why are business to business, government to government, and citizen to citizen interactions not included on slides 12 and 13 as needing authentication?
2. Are you also going to consider the privacy and security for patient and family members access to EHRs? Parents of adolescent children are a real challenge in some advanced EHR's like Kaiser or GHC.