

Privacy and Security Tiger Team
Draft Transcript
April 18, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director

Good afternoon, everybody and welcome to the Policy Committee's Privacy and Security Tiger Team. This is a Federal Advisory Committee, and there will be opportunity at the end of the call for the public to make comments.

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?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Carl Dvorak?

Carl Dvorak – Epic Systems – EVP

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

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

I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Micky Tripathi? Alice Brown for Christine Bechtel? John Houston might be off, but he's on. Wes Rishel? Leslie Francis couldn't make it. Sue McAndrew or Verne Rinker?

Verne Rinker

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Did I leave anyone off?

Neil Calman – Institute for Family Health – President & Cofounder

Neil Calman.

Judy Faulkner – Epic Systems – Founder

And Judy.

Judy Sparrow – Office of the National Coordinator – Executive Director

And Judy Faulkner, thank you.

W

And Judy, I'm here. This is ... sitting here for Joy Pritts.

Judy Sparrow – Office of the National Coordinator – Executive Director

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

Deven McGraw – Center for Democracy & Technology – Director

Thanks, everybody, for joining us both with respect to tiger team members and members of the public. On our agenda for today we're doing a little bit of a debrief on the Policy Committee meeting last Wednesday, which went very well. Then opening up our agenda a bit to talk about what issues members of the tiger team think we might want to tackle next because we've got a fair body of work that we've done to date. We have been operating with a lot of urgency on some issues that needed to be dealt with, either because ONC had an urgent need to get a response from us and some recommendations and/or we needed to squeeze some recommendations in to meet meaningful use and EHR stage two certification requirements to get into that pipeline.

We're now in the position of being able to sit back, not sit back but take a step back is probably a better way to refer to it, and think about what issues we think we ought to take on next. We don't have Joy Pritts on the phone with us today, she's on a much deserved vacation, but at least we can use the time that we have on this call to get some of the dialogue started. Then I think the other agenda item that we wanted to kick off, which is slightly new but related to the top two, is we have Deborah Lasky with us from ONC. They are eager to hear from us about whether there are areas of security policy where the public and relevant stakeholders might benefit from some additional guidance coming from the federal government. So we'll take on those topics today. We may not take up all the time on our call, but I think it's nice to have some breathing space to try to think about and get input on what our next steps might be.

Paul, I'm going to pause there and see if you want to add anything before we jump in.

Paul Egerman – Software Entrepreneur

I think it's a good summary.

Deven McGraw – Center for Democracy & Technology – Director

Okay, thank you. Essentially, the first topic is to debrief from the Policy Committee meeting, which took place last Wednesday, where we presented a set of recommendations on a number of issues, some of which were related to issues that we had discussed with the Policy Committee previously, but there were also some new ones on deck. Essentially, it turned out to be very successful. All of our recommendations were accepted. There was some dialogue and some questions, but it was fairly minimal. Neil, I recall that you raised a good point about how we keep setting minimum policy requirements and allowing entities to do more, which sometimes creates obstacles to interoperability down the road, which is something to think about. There were also some questions about some of the identity and authentication recommendations, which largely were due to some misunderstanding about what those two particular domains refer to, I think. But in general, again, it went very well. We didn't even use up all the time that we were allotted on the agenda and they were all approved.

Paul, I don't know if you want to add anything before we open it up to tiger team members who were present.

Paul Egerman – Software Entrepreneur

I'd just say that I think that was a good summary, Deven. All the recommendations were approved and I think that, as you said, Neil's comment is a good one. It's one of these things that in security what we intend to be a minimum can become the maximum in terms of either that's all vendors are able to do or it's just something to at least keep in mind that maybe we have to be careful of what the definition of minimum is. But I think everything was well received. I think the reason is for the most part these were recommendations that the tiger team had been already exposed to with the exception of the new information about patient portals. But other than that, the authentication material was material they had already been exposed to.

Deven McGraw – Center for Democracy & Technology – Director

Does anybody else want to share any thoughts or impressions from the meeting if you were either present or listening on the phone? It went that well. We were quite fortunate and very pleased that we didn't have necessarily any follow up work to do based on questions that came from the Policy Committee, which brings us to the second item on our agenda today, and that is where do we go from here? We have done a good bit of work on policies to flesh out a framework of policies focusing on the exchange transactions that are required for stage one of meaningful use, but yet we know that there are some other developments in the pipeline that are going to require some attention. Paul and I had a co-chair conversation this morning thinking about some issues that could possibly be teed up for our agenda over the next—we want to scope some things out for our meetings through the summer in order to continue to place ourselves on some meetable but nevertheless still present deadlines. Because I think we do our best work when we really force ourselves, quite frankly, to make some decisions on some difficult topics.

So we have teed up a couple for your consideration, one being the issue of corrections to data based on errors that are spotted either by patients or by other providers, and then the host of issues that arise with respect to different query and response models. Because again most of what we've done to date has envisioned more of a push transaction environment and now that there's an increasing focus on the query response model that may have been at least partially triggered by the release of the PCAST Report. But nevertheless they would have presented themselves one way or the other, sooner or later, but maybe further up on the agenda arguably due to that work and then opening it up really for discussion on those and other issues for tiger team members.

Paul, before we open up to the group I want to make sure I characterized—

Paul Egerman – Software Entrepreneur

You got it right.

Deven McGraw – Center for Democracy & Technology – Director

Yes, okay. Thoughts?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Deven, I have a question, I know Joy's not on the call, but are there any requests from ONC to provide input on any of the areas where they have a rule making obligation through HITECH and maybe these are issues that haven't yet been settled?

Deven McGraw – Center for Democracy & Technology – Director

There haven't been, I think in part because the rule making for ONC is the governance rule and my understanding from talking to Mary Jo Deering is that all of the recommendations that we've done to date have been feeding into that process. They've been watching very carefully what we've been doing in terms of the conditions of trust and interoperability for participation in the Nationwide Health Information Network. Then for the rules that the Office of Civil Rights is putting out, we don't directly advise them and

conversations that I've had with Joy to date, those are so far along in the pipeline that anything that we would do on those now might be too late—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

....

Deven McGraw – Center for Democracy & Technology – Director

... pronouncements.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Okay, so that includes accounting for disclosures and all these other things?

Deven McGraw – Center for Democracy & Technology – Director

Again, my impression from talking to Joy, and we have one or two folks from OCR on the phone, if they want to chime in, but I thought that the accounting of disclosure rule was already in regulatory clearance.

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

Deven, at the last Standards Committee meeting, that committee approved a recommendation from our committee to the Policy Committee. I don't know whether you've seen it, it has been officially transmitted to ONC, but the recommendation was that we need policy around how to establish the minimum trustworthy certificate of organization, certificate authorities that issue digital certificates to health entities maybe exchanging information using the direct exchange. Where how do you decide whether Certificates 'R' Us is a sufficiently trustworthy organization to issue those certificates?

Deven McGraw – Center for Democracy & Technology – Director

You know what, I might have been cc'd on an e-mail but nothing more specific than that has been brought to my attention. Paul, is this anything that you had heard?

Paul Egerman – Software Entrepreneur

I only heard it through Dixie. I think we need to tee that one up. That's a good issue. I understand what the issue is. That issue is probably part of a category of issues. I bet there were a lot of things that we put on the parking lot when we were going through a lot of these items. That may have been one of them that we really didn't consider.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Software Entrepreneur

We should probably review that. That's a good point, Dixie. Let's see if we can address that possibility in the next meeting.

Neil Calman – Institute for Family Health – President & Cofounder

Paul, that's what I sent you that copy of that article about, you and Deven, that was in *The Times*.

Deven McGraw – Center for Democracy & Technology – Director

Neil?

Neil Calman – Institute for Family Health – President & Cofounder

Yes, can you hear me?

Deven McGraw – Center for Democracy & Technology – Director

We can hear you. I'm just trying to—

Paul Egerman – Software Entrepreneur

There was—

Neil Calman – Institute for Family Health – President & Cofounder

Yes, there was—

Paul Egerman – Software Entrepreneur

... in the article.

Deven McGraw – Center for Democracy & Technology – Director

Oh, right, “An Attack Sheds Light on Internet Security Holes.”

Neil Calman – Institute for Family Health – President & Cofounder

Yes. Apparently, that’s what it was all about was all of the subcontracting that’s going on around issuing these certificates to the point where nobody’s quite sure what it means.

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

Good. I’d like to see that article.

Deven McGraw – Center for Democracy & Technology – Director

All right, I’m forwarding it.

Neil Calman – Institute for Family Health – President & Cofounder

Yes, if you can forward it to the whole committee.

Deven McGraw – Center for Democracy & Technology – Director

Will do.

Neil Calman – Institute for Family Health – President & Cofounder

Yes, there’s a big article in *The Times* about it—

Paul Egerman – Software Entrepreneur

Yes and—

Neil Calman – Institute for Family Health – President & Cofounder

....

Paul Egerman – Software Entrepreneur

It is a good issue, because if I remember correctly, I might have this wrong, is NW-HIN Exchange created their own certificate authorities. They did something special with the certificate authorities and we probably should look at how they handled that issue.

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

I can tell you how they handled it is that they do have their own certificate authority but that certificate authority for the NW-HIN Exchange is cross-certified with the federal bridge certificate authority. So by definition it has to meet the minimum standards for the federal bridge cross-certification.

Deven McGraw – Center for Democracy & Technology – Director

It might be helpful to have someone who’s knowledgeable about what those standards are to provide us some background information. Is that—?

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

Along with the transmittal letter, I know Judy’s on the line, but along with the transmittal letter we attached some slides that provide background information like this. Maybe I could just send those directly to you.

Deven McGraw – Center for Democracy & Technology – Director

Sure.

Paul Egerman – Software Entrepreneur

That would be great. Keep in mind what we're really trying to accomplish on this call is to get the list of topics. There's always a tendency to start talking about the topics, especially since they tend to be very interesting issues, so make sure we understand it. We put this down on the list. What we have so far on our list is there's an issue related to corrections, is that right, Deven, that we probably want to discuss?

Deven McGraw – Center for Democracy & Technology – Director

Yes. As you'll recall, when we were talking about patient access to data and particularly in the context of matching patients with the right information discussion and there was a fair degree of discussion about what ought to happen if an individual spies an error in the record. We didn't actually get time to reach closure on a set of policies around that, we initially circulated some materials about what the HIPAA rules require in that respect. But that's another one that we put in the parking lot because we weren't able to finish it in time for the Policy Committee's meeting. So I was resurfacing that one as well.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I just wanted to ask—certainly that is one issue but I heard you also mention where it I guess based on our first letter to the Policy Committee ... where we said we need to come back to looking at the policies and to the areas of the principles of ..., at some point, I mean, patient correction is one aspect of data integrity and quality, and I think it's an important aspect, but it's not the only aspect. Sometimes people will get erroneous information and it is matched with the right patient, so I guess I'm just wondering ... go back to that particularly because the FTC and the commerce report are out now and they're also, in terms of the general environment advocating a ... approach. I'm just wondering if we have a plan to go back through all the areas of the ONC principles and think through some of the holes that might be left for a push.

Deven McGraw – Center for Democracy & Technology – Director

Yes, that's actually what I was hoping we would do during this call. Which is why the framework document that we've been working on that has the ONC principles and fleshes out what current law provides for each of those principles in a summary way and then what our recommendations have been to date, again, nested within those principles, that's the document that we sent last Friday. So that is a better characterization, Carol, of what I hoped, a conversation that we would start today. Where are the holes? Part of that is that actually in ONC's principles they don't nest the correction principle within data quality and integrity. That's actually a separate principle in that regard. It is related to our overall goal of always trying to take a look at what ONC has put forth at a principle level and how do you flesh those out with policies. That's exactly what we're trying to do.

Paul Egerman – Software Entrepreneur

Carol, were you saying the first part is to say where the holes were, the missing parts, as it relates to these push transactions, is that what you were saying?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, I was saying I heard Deven say we might be moving on to query response and I guess I feel we still have some ... in the implementation or the specification of policies for the work we started on push, and I was just asking if we were going to close those gaps first.

Paul Egerman – Software Entrepreneur

Where do you see those gaps?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I think they exist in each of the principles to some degree based on what we know about push now. But I don't think we've touched on data integrity and quality. I don't think we've touched on corrections. I don't know that we have completely dealt with collection limitation and use limitation and some of those other elements of the framework. I'd be happy to go through each one, but I think it's an exercise that's worth doing in a methodical way. Because I don't know that we have covered the terrain in terms of specifying to a little bit greater degree much of the ... for the areas that have consumed our work the last couple of months, some of these other policies.

Paul Egerman – Software Entrepreneur

So what you're suggesting, let me see if I've got this right, is before we move on to query response what we ought to do is review the entire framework from a standpoint of these push transactions and in effect complete the framework and say, this is it. We've got a complete framework for push and now we're moving on to query response.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I think that's ideal. It's hard because push is In other words, once you pull through some of those things I think query response has a stronger foundation.

Deven McGraw – Center for Democracy & Technology – Director

Yes, and I'm not disagreeing with you at all, Carol. That's why I think it would be helpful for folks to identify gaps because not only are the push transactions easier to resolve, it's also the area that is better, it's covered relatively well by existing law. So it's both an examination of what are the principles, what does the law already provide, and then where are the gaps given that environment. I'm not opposed to it at all. I actually agree with you that we will have a foundation upon which to build policy for some of the more difficult query response scenarios. The foundation is strong. It doesn't have holes in it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that many of these issues are cross-cutting and will apply equally to push as well as query, and in some cases apply to the simplest thing of all, which is the record itself, like a right to a correction, something ... that you might access through a portal where there's no movement of the data at all.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Agreed.

M

However we frame it, we'll get into the meat of it.

Paul Egerman – Software Entrepreneur

The sense I have is, let me see if I can summarize what I've heard, is we want to review the entire framework from the standpoint of push transaction and see where there are gaps. Where we think there are gaps so far is in corrections, perhaps in some of these areas of data integrity and quality, collection limitations and use. We want to review that material with a goal in mind of saying, first we're going to complete the framework document for push transactions, then we're going to move on and work on query response. Is that a good summary?

Deven McGraw – Center for Democracy & Technology – Director

Yes, although I would say that we have been asked to focus initially on exchange transactions for the purposes under stage one of meaningful use versus necessarily taking on the secondary uses.

Paul Egerman – Software Entrepreneur

That's correct. When I said "push transactions" and "query response" I didn't really mean secondary uses at all. So that maybe it's an issue of understanding what it means like query response, but I was thinking entirely as query response related to treatment purposes.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Software Entrepreneur

Which might be, I don't know if that's more limiting or less limiting, but I picture, it's almost like we've got three stages here. One is push transactions. The second is query response for treatment. The third stage is when we get to secondary uses. I just think secondary uses is a different world.

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

Paul, would you consider also that the topic that we addressed in the PCAST actually of a persistence of privacy rules, would you address that along with secondary use? Or is that yet a different topic?

Paul Egerman – Software Entrepreneur

The persistence of privacy rules really should come through our framework, the portion as we do query response. It would just seem to me somewhere in there we're going to say patients need to be able to change their mind, but once they've said something that needs to persist until they change their mind and so somehow in there would be, I don't know if that's responsive to your question, but—

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

It is, but I think that we should write that down and make sure that we cover it.

Paul Egerman – Software Entrepreneur

Right. The purpose of doing the framework should be that we end up with a set of basic foundational or fundamental principles so that when we come to some of these issues, like your question related to the structure of the DEAS, we should be able to answer in the context of these fundamental principles.

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

Yes.

Paul Egerman – Software Entrepreneur

That should be what our goal is. In other words, the way I look at it is maybe this is an opportunity to feel like we're starting to catch up. In other words, up until now, it's almost like fighting fires. We've been responding to issues that were really urgent because we were trying to deploy technology, and now's a chance to make sure that we do what we say we're going to do, is make sure we have a foundation that we can build on that can make some of these things easier. Your question, Dixie, about the requirements for certificate authorities, well, that's not going to be one of the fundamental principles, but hopefully there's something in the fundamental principles that may help us, but you still have to respond to issues like that anyway. There's other policy issues that are not quite foundational that are tactically extremely important.

Neil Calman – Institute for Family Health – President & Cofounder

Paul, can I put another item on the agenda? I can't tell when you're finished with stuff.

Deven McGraw – Center for Democracy & Technology – Director

No, we're not. This is brainstorming here.

Paul Egerman – Software Entrepreneur

Yes, so go ahead, Neil.

Neil Calman – Institute for Family Health – President & Cofounder

I have no idea how we're going to deal with it. I'll preface this by saying, but our biggest concern, and I shared this with Deven a while ago and now it's getting even more of a concern, that is now that we're starting to be involved in exchanges, is unauthorized access of information by people who really have an intent to do wrong. These are people who are authorizing information on friends and for friends and we've had, I think, so far eight people that we've fired summarily in our organization in the last eight years since we've been doing this. But now that we're exchanging information we've started to have the same kinds of issues go on by people who understand that through our electronic health records they can now get access to information from hospital emergency rooms and from other places.

I keep trying to figure out whether there's a policy angle for this, whether there's anything that we can do around any kind of policy or standard. I only have two thoughts about that. One is it seems to me about roles something about the way roles are established in organizations. That if you have an organization where basically anybody can access the clinical information or information on diagnosis, including people who are billers, people at the front desk, etc., and you're exchanging information with an organization that

has much more restricted access with regard to roles. That you're as vulnerable as the person who's got the broadest expansive definition of what roles and who they allow to access what types of information.

I'm wondering whether there's some sort of policy angle here. We haven't really talked about this at all and that's why I'm reluctant to even bring it up, because I don't know whether there is one. But some people think about how roles are defined and whether or not we need to call something out about that, something that says roles have to be defined to be so that the minimum necessary for people to accomplish their jobs in an organization. The second angle is, aside from your threat of firing people, I just don't know what other angles there are to call out how serious an issue this is going to be. I think that for all the time we're spending with worrying about people accessing random heaps of information, the biggest threat that really exists for people is people who have a reason to want to access somebody's information and appropriately doing that. I'd throw that out as a problem without any real sense of what schedule solutions are or even whether it's within our purview to discuss that.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

If I might jump in here, I think, Neil, that is a perfect example of an issue that touches on several elements of ... overriding principles. It's clearly an issue that has to be addressed for trust in the network. If you believe your exchange partner is giving unfettered access or inappropriate access you're just not going to participate, so it's clearly an issue that has to be addressed from a trust perspective. But it's also an issue where a lot of people think about audit as a technical or security issue, but there's a whole set of policy issues that are related to audit which has to do with how the audit logs are used and monitored and how they're acted upon. That's an earlier stage even than dealing with it when somebody does the wrong thing.

I worry about the role-based approach, though because sometimes people in appropriate roles also do the wrong thing. It's by far one of the most common. It's the authorized user who does something wrong, and it's by far the most common way that information unfortunately gets breached. But it is an issue, it's a perfect kind of issue to dig into because a lot of elements of the principles have to be applied in order to address it appropriately, and I would argue even transparency, right? If somebody has had inappropriate access the trading partners want to know very quickly. I think all of these things are very related and it's a great example of why you really have to come at this from multiple angles, if you will.

Paul Egerman – Software Entrepreneur

Those are good comments, Neil, and good comments, Carol. Let me ask a question, Carol and Neil, this issue is predominantly when we get to query response, is that correct?

Neil Calman – Institute for Family Health – President & Cofounder

I think we're talking about it and not just related to exchange. It's a privacy issue related to the use of electronic health information that people have access to it. But I think with exchange it gets even worse because there's less accountability. As the network of people exchanging information grows larger and larger, it's harder and harder to provide that kind of assurance that Carol's talking about that all of the people that are in this trading network are trustworthy, and even how that's defined.

Judy Faulkner – Epic Systems – Founder

To add on to what Neil—I'm not sure, maybe you were still going. I might have interrupted you. Go ahead.

Neil Calman – Institute for Family Health – President & Cofounder

No, that's okay. I'm done.

Judy Faulkner – Epic Systems – Founder

Okay. One of the things we touched on at the Policy Committee meeting was the need to define providers better. Because, Neil, you may have the rules in your organization that a psychiatrist can see this, a physician who is not a psychiatrist can see that, a receptionist can see something, etc. But since the terminology for who is what provider is not defined across customers or across vendors, you can't let

that information go somewhere else and know that they will apply the same rules because of the fact that they're aren't the same coding schemes.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, and, Judy, I would say that role-based access, access control is a very difficult issue to implement even inside of an enterprise. Getting that right, implementing it right, and then making a lot of patients as the users change roles or come in and out of the organization, I mean, the largest companies in the world struggle with it, so it's a very complex remediation to really implement well in any sector.

Paul Egerman – Software Entrepreneur

Things that are complicated and difficult to do, that should be our job, really. I understand your comment, Carol. I understand your comment, Judy. But I think that we do good work for ONC when we address things that are very challenging, and sometimes you address it and you say that it's challenging and you can't do anything with it, or you say this is the best that you can do and it's not the whole picture or here are the alternatives. That's just an observation.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, if it's not hard, it's not worth doing. I agree with that. But what I was really trying to say was the perfect implementation of role-based access on its own is usually not enough. In other words, you have to think about this problem from multiple angles, as I was trying ... earlier.

Judy Faulkner – Epic Systems – Founder

Yes, and my point was simply we don't even have the basic bottom part which is defining it so that everyone's using the same definitions. But that's one of the things when Neil says going from one place to another we can't do that at all.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I know, Judy. But I'm struggling to think about how you have a common set of role definitions in a healthcare system that's characterized by widely varying resources. It might be that the nurse is the only other administrative person in the office with access to the record and in other places you can define the roles in a more granular way. I see this enormous challenge of setting policy benchmarks that are going to work in every organization.

Paul Egerman – Software Entrepreneur

Let's realize again what we're trying to do here is think through what our future agenda topics are, as opposed to solving them right now. So the point that Neil raises is a really excellent point, he's raising it from the perspective of a provider who's got experience with exchange and he says I've got problems with unauthorized access. So part of the response is yes, when we do query response we've got to deal with that from the standpoint of the So we've got to talk about audit and we've got to talk about some of these issues, including can you define roles, to what extent is that a viable approach, what are the challenges involved in doing that, and are there any solutions to mitigate those challenges.

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

I would like to weigh in on support of this particular topic as something I think is worthy of investigating. I do agree that it's not just being able to determine who should access what or log who's accessing what, but also a decision about how much access patients will have to understanding who's accessed a record as well as making it clear who's accountable for what institutionally for enforcement.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I would second that notion that accounting for disclosure is a really controversial and hard topic in terms of the trade-offs it forces between complete transparency to the patient with burden on the institution.

Deven McGraw – Center for Democracy & Technology – Director

Right, although, David, I'm not sure if you were here at the beginning of the call when Carol asked the question about whether we were, from a timing perspective, able to provide some recommendations that might influence the accounting of disclosure rule. I'm pretty sure that's already in regulatory clearance.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, so when we talk about transparency, what are we talking about?

Deven McGraw – Center for Democracy & Technology – Director

I think maybe if we stay out of the realm of specifically comment, I mean, we'll have to think about it. There may still be space to talk about it at a broader policy level without diving into the details of how one would implement the accounting of disclosure provisions that Congress enacted as part of HITECH, which are pretty down in the weeds.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. I don't know what authority we're making most of these recommendations under, for that matter.

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

Can I suggest that I think there's a fair amount of harmony here. I think the accounting of disclosure requirements are going to be, as Deven said, in the weeds. But they're also very much provider based, or covered entity based, and what we're talking about I think is as data flows across between covered entities, how are we going to make sure that appropriate accountings occur, in the fabric itself maybe is the best way to describe it.

Paul Egerman – Software Entrepreneur

What I thought I heard you say before, John, when you talked about patients, was not just accounting for disclosure, it was the concept of usability. In other words, how do you do this in such a way that it makes sense and it's usable for the patients.

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

Absolutely. It's huge and it could be either a big burden or a big opportunity.

Paul Egerman – Software Entrepreneur

Yes, because I've seen what a lot of these things look like and it's hard to figure it out. You've got some quality assurance person that's looking at a record and some administrative person and there are 30 people involved and it can be very confusing. It's hard for patients to figure out what is a routine administrative thing, a manager's looking over the shoulder of somebody, which is a reasonable thing to do, versus an example of the situation that Neil discussed, where there's somebody perhaps inappropriate looking at the record. I don't know how to say it, but it is an interesting issue of the usability of that for patients.

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

Yes, and I think the other thing too that we're going to find is that once data gets passed within the fabric, who the user is on the other end may be not even known to the HIE or to the exchange. But it's what institution is asking for the information. So you have almost this federated responsibility where you can say, okay, that data was requested by UPMC, so that level accounting may come from an exchange, whereas, then UPMC might have to be accountable within itself for describing who accessed that information once it was received.

Neil Calman – Institute for Family Health – President & Cofounder

Right. Let me just throw one more issue in here in response to one of Carol's comments about the trust fabric. This has been something else that concerned me in this whole thing. First of all, I think we should separate out what we're going to do to try to see if there's anything to keep people from inappropriately accessing information from all of the audit and disclosure conversations. From my perspective, I believe in prevention so I'd like to figure out if there's anything we can do that will help this on the preventive side before we get into lots of conversations about what we're going to do in terms of disclosing it. I think that that's a really important concept. But then, well, I'll hold my other comments for later. I guess I'm suggesting that we divide up the conversation into two parts when we have it. One is what we can do to prevent inappropriate access and the second is all of the things about how we inform people later on if their information was accessed.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think both of those angles have to be dealt with, but you need them both.

Neil Calman – Institute for Family Health – President & Cofounder

Agreed.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes. I would say, Paul, too, on the prevention question that many of the principles in ... were really designed for that. We've got an ... Connecting for Health, which was if you don't want to design databases for health information ... don't create a giant database of health information. There is something to be said for data minimization, collection limitation, use limitation. Breaches happen, but the extent of them and the scale of them can definitely also be mitigated with some careful policies. I think those are worth considering.

Paul Egerman – Software Entrepreneur

That's right. I think those are all good comments. I also like John Houston's comment about the usability of this information, though, for patients. I think about a situation a patient goes through when ... uses for exchange examples. The patient goes to the emergency room. If the patient goes to the emergency room there are going to easily be 20 or 30 people at that emergency department that end up accessing the record and what is really usable to the patient under those circumstances is possibly just that the patient's record got transmitted to the ED department. It's an observation. It gets even more complicated if the patient were admitted. There could be 100 people or more touching inpatient documents to make it usable to the patient, because otherwise the patient has to look at this and say I don't know who these 100 people are.

Neil Calman – Institute for Family Health – President & Cofounder

Not only that, for months later people can be accessing that information around billing procedures, follow up and all kinds of other things.

Paul Egerman – Software Entrepreneur

Coding information, all kinds of stuff.

Neil Calman – Institute for Family Health – President & Cofounder

Yes.

Paul Egerman – Software Entrepreneur

Chart completion.

Deven McGraw – Center for Democracy & Technology – Director

Carol, did you have another point you wanted to make?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

No, I was just going to agree that that is a big question and it raises the question, again, of what gets shared and what needs to be shared and the policies that surround that.

Neil Calman – Institute for Family Health – President & Cofounder

I was just going to follow up on Carol's thoughts about this trust fabric piece, which is a question for me too. If you have a breach like we did in our organization, or two, or three or four of them over a period of time, how are we going to deal with that in the framework of trying to understand what does that mean for my organization and participating in exchanges and stuff like that. Who's going to know about just those kinds of things? It's not a breach of 1,000 records or somebody stealing a data file, it's a policy inside my organization, let's say, that hasn't provided the greatest privacy for our patient's information.

So what happens with that, and I'm using our own organization as an example, but it could be anybody, so what happens to the organization? What is the process by which I want to remain a trusted part of this

network of people exchanging information? It's just not clear to me how that stuff plays out at the ground level, so maybe it's clear to others. If it is, it doesn't need to be on the agenda, but if it's not I think we have to think through what does it mean and is it just the providers, is it just one of the sites, is it the whole organization, is there some remedial process that goes on. I guess I'm not talking about the kind of ... disclosures that are being discussed as being publicly reportable, but now just organizations that don't have the appropriate policies and procedures in place or have the appropriate policies and procedures in place but have people that are violating them.

Paul Egerman – Software Entrepreneur

Are you talking about, are those responsibilities of record holders? Is that one way to summarize what you're talking about?

Neil Calman – Institute for Family Health – President & Cofounder

I guess, but also what does it mean in terms of what we're talking about this trust framework of people exchanging information. There's all these entities in it, and we want those entities to continue to share information, but we want them to do it correctly and it's not clear how that whole trust framework plays out at the ground level.

Deven McGraw – Center for Democracy & Technology – Director

It begs the question of whether the vehicle for enforcing a minimum code of conduct for exchangers is, or at least it helps to have the set of conditions of trust and interoperability for the Nationwide Health Information Network. So that you have to have minimum processes and demonstrate that you're implementing them in place in order to be part of that network and then if you're not there needs to be some consequences associated with that so that people can trust one another in the exchange process.

Paul Egerman – Software Entrepreneur

But where do we cross the line where we're not talking about privacy and security anymore and we're now talking about exchange governance?

Neil Calman – Institute for Family Health – President & Cofounder

Right, that's—

Deven McGraw – Center for Democracy & Technology – Director

I think it's not exchange governance, it's what does it look like and who's on the board, but what are the conditions of trust and interoperability that have privacy and security dimensions to them that then become part of the requirements for being able to use the brand?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Paul, I was actually going to say that I thought your question was really insightful from the perspective that there's been almost a knee jerk on some of the technical requirements that implement privacy and security on the certification of those requirements as was necessary to implement privacy and security. But where this conversation is I think is the right place, which is that privacy and security is really about, assuming the basic technical things are in place, it's really about people and entities and how they implement those policies and their behavior on the network. I think that's the appropriate focus for the privacy conversation. If all you had to do was use a system that has the technical capabilities for creating an audit trail and assuring the right role-based asset, life would be easy. But it's much more complicated than because this is about people.

Paul Egerman – Software Entrepreneur

That's right. So what I was trying to say responsibilities ... are really responsibilities, when I think about Neil, I think about Neil as an employer, as a provider that has a number of people working in his practice. So the issue is what are his responsibilities to monitor and make sure that things are being done correctly among those people?

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

I think he's also, don't let me put words in your mouth, Neil, but I think this is a really good topic. I think he's also talking about transparency between organizations. We talk about consumer transparency and what happens to the data, but if I as an organization send my patient's data over to another provider what kind of transparency am I supposed to get? If they then have an internal breach that discloses the information that I've shared with them, are they also responsible to let me know?

Neil Calman – Institute for Family Health – President & Cofounder

W my responsibility? So when somebody in the emergency room was asked by somebody who knew them to access records from our center and did, do I now have a responsibility to go to the hospital—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes.

Neil Calman – Institute for Family Health – President & Cofounder

—... that accessed that and say, let me see what your policies are, because somebody inappropriately accessed our information and I want to make sure that this doesn't happen again. Think about that in a national network framework, so that's what I'm really asking is how does it play, both for me as a provider and record holder of 100,000 peoples' records, but also as a participant in this framework, in this national matrix?

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

I think these are all fair game for this whole discussion. The other question, too, is what's the purpose of the DURSA and how does that fit into all of this?

Paul Egerman – Software Entrepreneur

Well, it's interrelated.

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

That's what I mean. And it's—

Paul Egerman – Software Entrepreneur

The issue is the purpose of the DURSA and is that kind of document effective?

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

Although some of this is going to come out in the governance ruling, I assume, which doesn't mean we shouldn't discuss it. But we may be overlapping that, which I assume is also fairly well along.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I assume so too. This is Deven. But we can do some inquiry on that. But nevertheless it clearly is the topic that people have strong interest in discussing. We can do a little background work to see if we're, from a timing perspective, well timed to insert them into an ongoing process. But nevertheless I think this one is one people have expressed a high degree of interest in, and I agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Can I change the subject to something we just touched on before and I want to bring it back up to make sure it doesn't get left off?

Paul Egerman – Software Entrepreneur

That would be great.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's just that going a little deeper on the data integrity question, we have put a fair amount of effort into protecting the data as it moves across connections, but I'm interested in having a discussion on actually protecting the data itself with a digital signature or something like that. The reason I think it's going to become more important is that as consumers have more and more of this data in their hands and present it to providers who maybe don't have access to it through any other way, how can the providers trust that

it hasn't been tampered with? So there's a lot of good technical ways to prevent that, but is it something that should be elevated up to something that could even be certified by the EHR vendors, the ability to sign the documents, for example?

Paul Egerman – Software Entrepreneur

It makes sense.

Deven McGraw – Center for Democracy & Technology – Director

It does make sense. What did we say in the recommendations we just did on the portal, that there would need to be provisions for data provenance and we acknowledge that more work would need to be done both from the perspective of what exactly ought to be included and what's the technical mechanism for making that accessible or viewable. But we just put a placeholder in for that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, I agree. It's more setting the expectation that this would be something that should be done. It's something that can be done today, but it's not being done by hardly anyone. I think as copies of the record proliferate and the consumers control, or through consumer designated entities like a personal health record, providers have already raised to me the question of how can I trust that data? I think it's a policy question, because we know how to protect it technically.

Paul Egerman – Software Entrepreneur

Okay, that's a good topic. Any other topics people want to raise?

Deven McGraw – Center for Democracy & Technology – Director

This is not your last bite at this apple, because I suspect that maybe folks didn't have a chance to re-look at the framework document and orient themselves to raising particular details. We're also going to post this on the Health IT Policy Committee blog to get some input from the public as well.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Good idea.

Paul Egerman – Software Entrepreneur

What about on the security side? I've been thinking about this a lot in terms of privacy, but one of the things I think ONC is asking is are there any gaps in what we said about security?

Deven McGraw – Center for Democracy & Technology – Director

Right, although is this what Deborah Lasky talked to us earlier about, Paul?

Paul Egerman – Software Entrepreneur

Yes, it is.

Deven McGraw – Center for Democracy & Technology – Director

Because it's also about guidance versus additional policy.

Paul Egerman – Software Entrepreneur

That's correct.

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

That data integrity is sort of a security issue.

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

It's definitely a security issue.

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

Okay. I wouldn't have said it that hard, but, yes, I agree.

Paul Egerman – Software Entrepreneur

You said that so affirmatively I would be forced to agree with you too. I have no idea. Where are there gaps in security that we should be giving guidance to ONC about?

Deven McGraw – Center for Democracy & Technology – Director

Then on the flip side of that is there's no clear area where additional policy is needed, what are areas where it would be helpful for ONC to provide stakeholders directly with some additional guidance about how to comply with existing policies?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I definitely think the audit area is one. It's just that it's not the audit function of the security item, but it is the use of the ... of that log and the timeliness of it, because very often it's there, but it takes some time to use.

Paul Egerman – Software Entrepreneur

Okay.

Neil Calman – Institute for Family Health – President & Cofounder

Paul, to your question, we just did give some recommendations that are related to security, such as encryption, so it's not like we have been sitting in our hands.

Deven McGraw – Center for Democracy & Technology – Director

No.

Paul Egerman – Software Entrepreneur

Let me ask a couple of questions about this. One is, are there special security issues that should be considered when there's what I call concentrations of multiple entity data in your one location? So when you have large hosting facilities that may have hundreds of EHR systems in one location. Or even when you think about the concept of the DEAS, where you have significant concentrations of protected information in one place, does that create— Because as more information doesn't, does that mean that there's potentially more risk and as a result there needs to be a different approach to security?

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

I think, Paul, that in this day and age the data are unlikely to be in one place, which raises the issue of are there security considerations around virtualization and cloud computing that we should be addressing, and I would say yes.

Paul Egerman – Software Entrepreneur

I disagree that it's unlikely to be in one place. There are a lot of hosting facilities where that exists, that have significant concentrations of data in one place. You can think about it as virtualization and cloud computing, but in point of fact there's simply a hosting facility with tons and tons of data ... place, because it hosts multiple electronic health records.

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

Yes, but also data centers increasingly are using cloud computing themselves, and I happen to think that cloud computing adds security as well as introduces new considerations, but I think that the rapid growth of the use of cloud computing may put it on our radar screen.

Neil Calman – Institute for Family Health – President & Cofounder

To me cloud computing is nothing more than, frankly, outsourcing, because that's been going on in large quantities for many, many years. It's always been handled, at least up to today by individual entities through their contractual relationships and business associate agreements with these facilities. I guess the question is, above and beyond having effective business associate agreements and ensuring that they apply to the HIPAA security rule, I'm not sure what else these third parties should be doing.

Paul Egerman – Software Entrepreneur

The way I look at it is you know ... if you ran a grocery store, you have a cash register and you have a certain amount of cash. So you have some security around that, but if you're a bank you have more security because you have a lot more cash and presumably you're a magnet for evil-doers because there's a lot more stuff there. But if you're Fort Knox or the New York Federal Reserve, where you have significant reserves, then you have even more security.

Neil Calman – Institute for Family Health – President & Cofounder

I'll give you an example, Paul, we've got Cerner, we have Siemens, SMS, that historically for years outsourced hospitals' EHRs, I know there are many others, I don't know if Epic does it, but there are many, many EHR providers that do significant massive outsourcing. I don't think this is a new phenomenon and I don't think it's been one where there has been an issue to date, I guess is my point.

Paul Egerman – Software Entrepreneur

Whether or not there's been an issue, my question is, is concentration of data in one location, is that a security issue that we should be giving guidance to ONC about?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes. Paul, if I could try to just offer one point of clarification. I think concentration is an issue and we know ... who have walked out physically with the servers, right? That's one mode. But one thing that might be clarifying to this conversation—because I agree that the host data has so evolved over the last couple of years that it's really important that we talk about “centralization” in a way that doesn't ... physical centralization. That is, I have one data center, versus logical centralization, which is that across that data center and across all of my sources of information, whether it's the ten providers I've seen out of the four hospitals I've been to and the six labs, whether or not there is ... centralization of that information ... is a breach of my ... physical centralization. Which arguably has some physical structural issues related to ... but the breach is potentially mitigated if it's not logically oriented, if that makes sense. I know maybe from a hosting perspective this has been all of the objectives, but certainly from the HIE perspective this is a question that comes up a lot.

Paul Egerman – Software Entrepreneur

Sure, because you've got to look at the architecture of the DEAS as opposed to the PCAST Report and there's a significant concentration of information in one physical location as it's proposed, and so I think that has additional security implications.

Carl Dvorak – Epic Systems – EVP

Paul, I would just add a comment that I think you're on the right track. When you give your data over to another entity to manage it for another set of purposes, then I do think I agree with you that additional requirements might be in order, so an HIE or a DEAS could definitely benefit from additional requirements. But I definitely agree with John on the hosting side, and I don't think size is the important thing there. Kaiser's got 8.5 million members and a Waco family practice might have 50,000. So I don't know that it's necessarily the concentration of data or the size of the data site, and I think cloud computing is today's name for software-as-a-service from yesterday, is the name for application service providers the year before that. It's the same thing as it was fundamentally 15 years ago or 20 years ago. The only thing that's really changing is the name. But in terms of interacting with them and working with them, they're very much the same as they've been the last several decades.

Paul Egerman – Software Entrepreneur

The way you would view this is a significant concentration is you're delegating your security obligations to somebody else and in those circumstances that's an issue that should be reviewed. Is that what you're saying?

Carl Dvorak – Epic Systems – EVP

I agree with John. I think hosting is the same as it has been since I can remember, since I was a kid, so I don't feel the need to do anything different than we've been doing. I think what we've been doing actually works very well, and it's only if you turn it over for a different purpose or a different use of it to an HIE or to a DEAS or to a marketing company there you might want to do something differently, but not for hosting.

It's not a function of size or how much data is there. A large organization might have more patient records in house in their own data centers than an aggregator or a hosting service. It's not about the concentration of data.

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

The software as a service issue may raise some additional security policy issues as well, because we expect a lot of small providers to use software as a service and by EHR access as a service, which is a good thing. But the separation of responsibility with respect to security between the software as a service provider versus the subscriber may be worthy of some discussion. When you buy software as a service you obviously can't assume that the service provider takes responsibility for all of HIPAA compliance, and it might be worth exploring what's the responsibility of the subscriber versus the provider.

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

To dovetail what Dixie just said, not all software as a service providers are the same. In fact, I would swear that some vendors get into the software as a service industry because their software isn't stable enough to have the customer run it at their facility. I can tell you from my experience running a large security organization that we have had our challenges with small software as a service providers and the fact that they don't have the level of sophistication sometimes that they really need to have.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But wouldn't the software as a service provider to a covered entity have a business associate agreement that puts them under the HIPAA extensions of HITECH. It wouldn't. I'll tell you what the dilemma is with that, is that when you're a large provider and you have hundreds of these and trying to police them adequately is very difficult. Now, there's something called high trust, if all these software as a service providers were required to meet the high trust standard and in essence go through a SAS 70 type of review as a requirement, that might raise everybody's level of trust in these software as a service providers.

Paul Egerman – Software Entrepreneur

What I'm trying to understand from this discussion, software as a service, let's use that as an example, is that a security issue that we should be marking as a topic that we want to discuss?

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

I think HIPAA with respect to software as a service and how the allocation of responsibility comes down might be worthy of discussion. As John just said, I know of examples as well, now that healthcare is starting to attract a lot of money these fly by night software people who don't know anything about healthcare are starting to offer software as a service and they don't necessarily even understand the basic requirements, some of them, of healthcare. I know of one instance where they get a software upgrade and overwrote the whole database and patient data wasn't available the next day. So the responsibilities for software as a service providers, I think are a bit different from provider organizations where HIPAA is all contained within the organization.

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

Can I suggest that if we're going to take this one on, which I think is worthy, that we recognize the fact that providers themselves can't each individually police all of these different vendors individually? What you have to do is come up with a framework where these vendors have to go through some type of certification that then all the different covered entities can rely upon when they choose one of these vendors to work with.

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

Yes.

Paul Egerman – Software Entrepreneur

Okay, good issues. Any other issues that we want to talk about, privacy or security?

Deven McGraw – Center for Democracy & Technology – Director

I think we've got a pretty good list going, but, yes, we definitely want to—

Paul Egerman – Software Entrepreneur

We've got enough to keep ourselves busy for one or two more meetings.

Deven McGraw – Center for Democracy & Technology – Director

Yes, more like ten.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The news was filled over the last couple of days with the White House's re-pushing the National Trusted Identity Initiative. That's something to put in the back of our list maybe for something in the future if that evolves to see if there's opinions that we have about its use in healthcare. I know we've already issued thoughts about identity proofing and authentication, but if the White House keeps pushing this NSTIC or whatever people call it, it will get referenced back to healthcare at some point.

Deven McGraw – Center for Democracy & Technology – Director

David, we did actually mention the need for ONC to provide guidance to providers that incorporated some of these developments, including, I've heard it referred to as NSTIC.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

NSTIC, yes, there you go. That's as bad as NW-HIN.

Deven McGraw – Center for Democracy & Technology – Director

It's nice to know that there's another industry that's stuck on acronyms other than healthcare.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It sounds like a finger stick or something. Anyway, I'm guessing that there will be a flurry of interest in it and it's something that questions may get asked about its role in healthcare.

Deven McGraw – Center for Democracy & Technology – Director

Right. Good point.

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

One more topic I might mention is accountable care organizations, ACOs, and whether there are different security and privacy policies for ACOs versus HIEs.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That's an interesting question. Accountable care organizations will push the boundaries of data sharing harder than anything else has done so.

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

Yes, because they absolutely will be looking at clinical information.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Paul Egerman – Software Entrepreneur

The response to that is maybe they will. They might push it within their accountable care organization, but they may actually put up barriers outside their accountable care organizations, because if they have fiscal responsibility for the patient they may have a disincentive to have the patient go outside the accountable care organization for care.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But the patients have the right to change organizations, at least under the current proposed rules, which means the data has to flow with the patient in some way, which will put stress on that private barrier. But I agree with you, Paul, that's very likely to be the way it starts.

Carl Dvorak – Epic Systems – EVP

Paul, I'm not sure how it will work in the end, but I was just at AMGMA and there was tremendous dissatisfaction with the ACO legislation. One of the things that they mentioned in particular was this notion of retrospective attribution. That the 5,000 patients, so if you make yourself an ACO you don't actually get to ... patients, the CMS folks will decide which 5,000 patients you had the most E&M exposure for and those will be the patients that count as part of your ACO. It won't be that you create a panel or recruit patients into it based on compliance or anything like that. You wouldn't know until after the fact who you were held accountable for. I'm not sure how that affects this topic. I think it was you, John, that suggested patients will have disincentives or incentives. I don't even know if patients will know they're part of it.

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

The patients continue to have completely free choice in the model.

M

Which means the data has to flow across all sorts of boundaries.

Deven McGraw – Center for Democracy & Technology – Director

Right. But what unique exchange issues are raised beyond the ones we've been struggling to deal with just because it's an ACO?

Neil Calman – Institute for Family Health – President & Cofounder

I think that people are going to be monitoring and trying to capture as much information as they can on the people who are their regular patients. Even though we're not going to know exactly who's going to be attributed to us, we're going to know 90% of them. So it's based upon what happened in the prior year and also the people who are continuing to use our services. So there's no question that the providers are going to be trying to accumulate as much information as they can about where people are going for care, and I think there's some pretty huge ... demand on the information exchange processes.

Deven McGraw – Center for Democracy & Technology – Director

So maybe not unique issues surface, this is Deven, but maybe surfaced in a time frame that's more rapidly approaching than we might have predicted.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And with more powerful business drivers than have been apparent for HIEs to date.

M

And not necessarily with the patient having been in your office to get a consent, which is a whole other issue. If there are people who are being attributed to you and you want to do outreach to them or try to accumulate information, trying to go through the whole process of getting consent to do that, not necessarily related to their immediate care needs is going to be another issue that we've been trying to address. You're not just getting the information about where they're going because you're interested in finding out, they were just hospitalized and you're following up and you're interested in looking at their entire spectrum of services, and you can go beyond what their immediate care needs are.

Paul Egerman – Software Entrepreneur

It makes sense. I think this has been a good discussion, Deven.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Software Entrepreneur

I'm afraid to ask for any more because ... us.

M

You'd better end the meeting early.

Deven McGraw – Center for Democracy & Technology – Director

Yes, and in reality, again, it doesn't preclude folks weighing in off line, but this exceeded my expectations in terms of the thoughts that people had, their good ones, most of them very hard issues, and Joy will be either pleased that we've got such a robust agenda for moving forward, or frightened by it. I think we did pretty well.

Paul Egerman – Software Entrepreneur

So do you think we're ready to open ourselves up for public comment?

Deven McGraw – Center for Democracy & Technology – Director

I think so. Let me just make sure, Deborah Lasky, Catherine Marchisini from ONC, did you have anything that you wanted to add or ask?

Deborah Lasky – ONC

I found the list of topics emerging to be really good ones and robust, and issues that we've been talking about actually here within ONC. So we're looking forward to hearing some more from the tiger team.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Deven, I just have one question, I don't expect that we can answer it, but I'm wondering, policy and many of the issues we've been discussing is a journey and not a destination, in that you're really never done. ... everything we talked about today, things evolve, things change, and there's more complicated issues to deal with, but one question I have is what is, and maybe this is a governance issue, I don't know, but the long term forum for that and where that lives is certainly a question I have.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I think it's a good question, Carol. I actually don't have the answer to it. I need the answer to it too. I certainly have presumed—at least since the Policy Committee went through the process of having a governance workgroup and getting some recommendations. And determining that they needed to put a proposed governance rule out in order to comply with their HITECH obligations—had always presumed that that might be the process going forward for the continual feedback loop that's going to ultimately be necessary for long term policy development and implementation in this space. But even if we were to all agree and ONC were to tell me I'm right that that is the vehicle beyond of course the legal piece that's in HIPAA and the evolution of that particular set of policies, it's hard even to speculate as to whether that's a good idea, whether it's going to be sufficient without seeing the rule. And of course we're still trying to influence it even as we are anticipating its release. We will have some conversations with Joy about that when she gets back from vacation, because I think it's a really good question.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

The work is never done.

Paul Egerman – Software Entrepreneur

That's right.

Deven McGraw – Center for Democracy & Technology – Director

All right, so let's open the lines for public comment, please.

Judy Sparrow – Office of the National Coordinator – Executive Director

Yes, anybody who wishes to make a comment, operator, can you let them know how to do that?

Operator

Yes. You don't have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director

Great, thank you. Thank you, Deven and Paul. It was a good call.

Deven McGraw – Center for Democracy & Technology – Director

Yes. Thanks for everyone's input. It was terrific.

Paul Egerman – Software Entrepreneur

Thank you. Happy Passover.

Deven McGraw – Center for Democracy & Technology – Director

Yes. Happy Passover.

Paul Egerman – Software Entrepreneur

Thank you.

Public Comment Received During the Meeting

1. NIST has fantastic information on CLOUD - Security, Privacy, Governance, etc

<http://www.nist.gov/itl/csd/cloud-020111.cfm>

2. Note that Digital Signatures are great technology, but the policy and administrative burden should not be overlooked <http://healthcaresecprivacy.blogspot.com/2010/11/signing-cda-documents.html>

3. How are the Privacy Principles weighed against Medical Records Retention, Community Health, Legal Discovery, etc?

4. Note that Healthcare Certificate management is not the same as Internet Browser Cert management

<http://healthcaresecprivacy.blogspot.com/2011/04/ssl-is-not-broken-browser-based-pki-is.html>

5. www.NSTIC.us; www.nist.gov/nstic/

6. With regard to "the Tiger Team determining what issues it should tackle next," consideration should be given to the initial charter and tasks placed before the Team when created, as explained succinctly on the Team website, as follows: "The Office of the National Coordinator for Health IT (ONC) has organized a workgroup (subcommittee) under the auspices of the HIT Policy Committee to move forward on a range of privacy and security issues. A new Privacy & Security Tiger Team (composed of members from the HITPC and the HITSC as well as NCVHS) will work over the next few months to address the requirements of HITECH and the needs of many new organizations created under that law. We expect the work of the Tiger Team to be completed by late fall 2010."