

**HIT Policy Committee
Privacy & Security Tiger Team
Transcript
April 15, 2013**

Presentation

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good afternoon everybody. This is MacKenzie Robertson in the Office of the National Coordinator for Health IT. This is a meeting of the HIT Policy Committee's Privacy & Security Tiger Team. This is a public call and there is time for public comment built into the agenda. The call is also being recorded, so please make sure you identify yourself when speaking. I'll now go through the roll call, once I open my roll call page. Deven McGraw?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Deven. Paul Egerman?

Paul Egerman – Businessman/Software Entrepreneur

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Paul. Dixie Baker? Neil Calman? Judy Faulkner? Leslie Francis?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Here.

MacKenzie Robertson – Office of the National Coordinator

Great. Thanks Leslie. Gayle Harrell? John Houston?

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

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks John. David McCallie?

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

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks David. Wes Rishel?

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Wes. Micky Tripathi? And Kitt Winter? Okay, with that I will turn the agenda back to you, Deven.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay great. Thank you very much. On deck for our call today, we'll spend a little bit of time at the outset debriefing what occurred at the Health IT Policy Committee last week where we presented most of our recommendations on Query. We will then proceed to try to wrap up discussion on the last issue on Query that we did not have time to finish. And then, assuming that we are able to wrap that up in this call, we will begin our next item on our sort of topic areas for the year, and that is, our responsibilities to digest the comments that came in on the Request for Comment, for some proposed objectives and certification criteria for Stage 3 of Meaningful Use. Each of the Policy Committee's working groups is tasked with going through those comments that are relevant to their particular issue portfolio, and so we don't have all of the comments, but we do have some of them to talk about.

We'll start that discussion with a sort of summary of the comments that came in, and Kathryn Marchesini from ONC will take us through some slides that summarize those comments. But for those of you who want to see all of those comments, all of the ones that are relevant to the topical areas that have been assigned to us, we actually sent them to you. And that's the reason why you had 12 attachments to the email that you received this morning for today's call. There was absolutely no expectation that you would have read through any of those documents in advance of this call, and in fact ...

M

Now you tell us.

M

It's the same thing I was going to say; now you tell us.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I'm sorry. No, you'll be way ahead of the game if you've already started reading through them. But, that's really background material for folks who want to understand in some more detail the particular responses of folks who submitted public comment. In fact, you can even see the identity of the people in the organizations who submitted those comments. Kathryn's summary will be much more high level, and again, at the summary phase. So, we've got 90 minutes on the call today. Paul and I will be both be on for the first hour and then Paul will take charge of the discussion beginning at 4, because unfortunately I had a calendar conflict that I could not move. So, my apologies for that, but I'm leaving you in very good hands. Paul, do you want to say anything before we jump into the first agenda item?

Paul Egerman – Businessman/Software Entrepreneur

No, I think you covered it well Deven. I would just, for anybody in Massachusetts, wish them a Happy Patriot's Day.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Oh, yes. Thank you very much and happy Tax Day to everybody else.

W

Are those two inter-related?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Uh, maybe. All right. So the first agenda item, let me see what we have, is to talk about the Health IT Policy Committee and our recommendations on Query Response, and they were very well received. We had some good discussion on a couple of the issues, in particular the issue – the policy issues around when data holders automate their responses and under what circumstances does that trigger meaningful choice. But I think basically we got consensus agreement on all of the recommendations that we teed up to the Policy Committee, which included for scenario 1, which is targeted query with, for non-sensitive data. All of the different questions that arose within that scenario, there were sort of 6 different questions that we teed up, and our responses about what would be reasonable in terms of a response or what would be reasonable to include within a query, we got through all of that. We also got through scenario 2, which is targeted query for direct treatment, but in circumstances where there are stronger privacy rules that govern. And then with respect to scenario 3, we dealt with the question, and this is scenario 3, as you might remember, was really dealing with non-targeted query, where you don't know who the patient's providers are, and you're looking for the patient's record. And our recommendation about whether meaningful choice should be required, in terms of whether a patient would or would not be included in an aggregator service that permits queries, we said yes, the Policy Committee agreed with us.

And then we asked for input on a second question related to this scenario which is, should querying entities be required to limit their queries in some way, such as by geography or by a list of providers or by some other factor. And we asked for specific Policy Committee input on this because as you'll recall, in our previous Tiger Team calls, we really didn't get a sufficient amount of time to get to this question. And, unfortunately or fortunately, depending on how you look at it, the Policy Committee was so interested in all of the other recommendations that we teed up, that we didn't really get any specific feedback from them on this particular question. And they wanted us, the Committee wanted us to deliberate on this one a little bit more and come back with something more specific. And that is our first item on the agenda today, which is to deal with this scenario 3, non-targeted query for direct treatment purposes. Again, this was the question that we did get approval on regarding meaningful choice of the patient to be included in an aggregator service. This is the question that we want to deal with today, which is whether querying entities should in some way be required to limit queries, such as by geography or list of providers. And, is Judy Faulkner on the phone?

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Yes I am.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Oh great. I didn't give you much notice that I was going to call on you today, but I'm hoping you're okay with that.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Sure.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Because I think it would be helpful to hear how this is handled in some other networks and we'll – I'll ask you to cover this. But then we'll of course open the call to the experience of other Tiger Team members, in terms of networks that they work with, in terms or whether you can query network wide or whether there are some limits, and what would be the reasons for placing limits, etcetera.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Okay. I'm in the car right now; I'm just reaching my office, so I'll be gone for a minute as I run from parking into the office.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Oh, okay. Do you want us to come back to you then?

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Yes, get back to me in a few minutes, because I'll run in.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay, no problem.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

All right.

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

Deven.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I think the way that we initially sort of posed this to the Policy Committee in terms of sort of prompting some additional discussion from them was, on the one hand you can understand that in an emergency situation, where you're really trying to find information about a patient and you don't really have a good idea, other than maybe an assumption that they're likely getting care in a geography where they live. But that's not a foregone conclusion, especially in a place where people frequently vacation, for example. In an emergency situation, the ability to query beyond a geographic area and without necessarily any limits could be potentially very valuable. On the other hand, permitting sort of a potentially nationwide query, in the case of a nationally available network, arguably might create scenarios for mischief. But you see, we don't really have any straw answers here, in part because we wanted to sort of generate some discussion among the Tiger Team members about whether this is something, in fact, that we should have a policy

recommendation on, or whether in fact the networks and their participants should essentially make these decisions, based on their own best judgments.

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

Deven, this is David. I dropped off the call for a brief second, some kind of a phone glitch. Did we answer the part 1 of this one sufficiently for no more discussion?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

We thought we did, David.

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

Okay. So, that's the meaningful choice about participating in the said network, right.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Right. Right.

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

So do you want to wait for Judy or do you want opinions to flow?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

No, we should begin discussing. Judy can join us when she is able to get inside.

Paul Egerman – Businessman/Software Entrepreneur

So this is ...

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

Okay. So I would say that the primary driving question is who's enrolled in what kind of a service and that we've addressed that, with the meaningful choice caveat, which is our core principle that we keep coming back to. And then beyond that, it's just kind of random whether or not the patient – the necessary data might be local or might be a particular list of doctors, and to put constraints on the system for those sort of arbitrary constraints, when you've already passed a meaningful choice hurdle, seems – it might make you feel good, but it's actually just random.

Paul Egerman – Businessman/Software Entrepreneur

This is Paul. Let me give you a couple of examples to try to make sure we understand the question that we're asking. You could think of a situation where a – say a patient goes to an emergency room and they say the name of my physician is Carl Jones, and maybe there are three medical groups in the state that have a Carl Jones in them. So, can the emergency room just ask all three if they have records? So what happens if the patient says, "My name is – my physician's name is Dr. Jones, and there's like maybe the emergency room is located in New York City and there's like 300 medical groups or locations nearby that have a Dr. Jones in them. Can they – 300?"

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

So are you saying, Paul, that the real question here is the patient matching accuracy problem? I mean the reason to limit this is to ...

Paul Egerman – Businessman/Software entrepreneur

Well, patient matching – it's just inquiry.

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

... try to improve accuracy?

Paul Egerman – Businessman/Software Entrepreneur

No, you've got to think about it from an inquiry standpoint. From an inquiry standpoint, if you look at the first example I gave, like the patient says my cardiologist is named Carl Jones, you know, you can imagine how you could like telephone the three medical groups that have Carl Jones in them, and see if you have...anybody has any data that helps you with that patient. And again, not necessarily even go through a locator service. But the person says, Dr. Jones, you could also just set up your computer system that it searches every single EHR system in like a 1,000-mile radius, of anybody, any physician that has Dr. Jones and see if the patient is there. And the question is, is from a policy standpoint, should that be allowed? Or you could ask the – you could check every single EHR system in the country.

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

But I think that boils down to what mechanisms are in place to ensure accurate matching of, in your case, providers, but probably more important in the long run, of patients. And that's an important independent question, because I'm not sure that an arbitrary local constraint is going to help you for someone who's travelling, for example. And it's just as likely to hurt you, as it is to help you. And increasing accuracy of matching, you can do that by reducing the denominator so you have fewer choices, but in the long run, you've got to do a better job with matching algorithms.

Paul Egerman – Businessman/Software Entrepreneur

You're focusing on the fact that I used the name Jones as my example.

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

Well, that you were – I thought you were positing a situation where you weren't sure which one was the right person.

Paul Egerman – Businessman/Software Entrepreneur

No, it's more an issue of you don't know where the record is located.

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

I thought this was in a non-targeted query; there might be a record locator service, so that you would go through that record locator. I thought that's what we were debating; I may have missed the question.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

No, that is the scenario.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

This is Wes.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

We're supposed to be debating, which I think the other thing that's throwing us off a little bit Paul, about your example, is that you have some idea of who the providers are, you're just having trouble finding them.

Paul Egerman – Businessman/Software Entrepreneur

Right.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

This is Wes. We seem to be – I think David and I are thinking along the lines of is he talking about technical difficulties doing the search or is he talking about inaccuracies – but I think the question has to be somehow stated differently. The question is, is there a policy objection to being able to search nationally for patients records, period, right?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, I think that's another way to frame the question Wes.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Made it safe.

Paul Egerman – Businessman/Software Entrepreneur

That's another way to frame it, that's a better way of framing it, so thank you Wes.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Okay.

Paul Egerman – Businessman/Software Entrepreneur

It's more like, can you just do like a really broad search and look a lot of places for a record.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

For a given person's records, for getting patient's records.

Paul Egerman – Businessman/Software Entrepreneur

For a given person's records.

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

Or for information about that person's record, you might not be searching the records directly.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Right.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Right.

Paul Egerman – Businessman/Software Entrepreneur

Just look everywhere.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

This is – I'm back on if you want me.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay. Thanks Judy, go ahead.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Okay. What we do is, we ask the patient where the patient has been seen, and by the way, this works very well. We ask the patient where the patient has been seen, and then we do a patient match checking between them – that place and us. So if I say that I've been seen at Group Health, then UW knows to get my record from Group Health. That works well. Now what we're doing in the next six months, what we will add on to this is places nearby, so the patient may say, Madison, Wisconsin. And then it would go...so basically what I like about this is, it is the patient's permission, Madison, Wisconsin, and then we can search everywhere within wherever a customer has defined, so that if they say it's 100 mile radius, we'll have a 100 mile radius around there. And then, we're also doing near where the patient lives and works, again with the patient's permission, but ...

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

But you don't ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

We don't do the entire – we do not query the entire countrywide network.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

What was the rationale for deciding that you would not do that, if you don't mind me asking?

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Well that's a good question, what was the rationale? I think it made sense to say to the patient, where are you coming from. And then it also is inefficient to have so much more data than you need. We have like a hundred – if you look at current patients it's about 155 million. If you look at the entire databases, we have several hundred million, so, you're going to get an awful lot of false record matching if you do that. Whereas this way, you're much more pointed to the patient who's saying, here's where I've been seen.

Paul Egerman – Businessman/Software Entrepreneur

Yes, and so Judy, it sounds like one of the ...

W

The other ...

Paul Egerman – Businessman/Software Entrepreneur

Motivations might be to not burden the institutions with a lot of traffic that is not likely...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Exactly.

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

But there are other technical approaches that would alleviate the inefficiency and would increase the accuracy of the match to the point where that's not the primary concern.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Well we do have a very high match, so we're not – that's not a big problem that we've run into.

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

Right, but I'm saying it is possible to build national scale MPI services that match with high accuracy, that's what Surescripts does, and when you query Surescripts there's no location restriction to pharmacies nearby or anything like that, they match you against a full database. And it works pretty well, obviously, since it's a very successful service. So I'm saying that the technical reasons to not want to blast out a query to a lot of nodes is a valid technical issue to deal with, but the – it can be dealt with through indexing and through ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Oh no, no, I'm not saying the nodes, I'm saying that if – I don't mean that. I just mean that there's an awful lot of matches that you're going to get to Judy Faulkner, if you go worldwide and there are very few, and I think we have to consider worldwide eventually, not just nationwide. And there are very few if you go to just the areas that the patient says, this is where I receive my care.

Paul Egerman – Businessman/Software Entrepreneur

Right.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

And I also like the fact that it gives meaningful choice for the patient.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

This is Leslie Francis.

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

And so, this is David again, I mean I think that's ...

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay, hold on a second, I just – folks that haven't in the background and haven't had a chance to break in, was that Leslie or Kitt or both of you.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

It's Leslie, yeah.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

I'm where it's hard for me to talk and I just wanted to say that one of the issues that we heard about at NCVHS was the worry on the part of patients who are being stalked, that national searches would be a way of turning up, of course by unauthorized people, but that's still why you want to worry about patient consent. And so the kind of policy that Judy has allows for patients who are worried about that, to be able to put that kind of limit on.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay. Thank you Leslie, that's helpful to know. All right, David, thank you for allowing me to interject, I just – I kept hearing little voices in the background and I wanted to make sure we weren't steamrolling over folks so.

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

So, should I pick up, or do you want to keep going around the table?

Deven McGraw, JD, MPH – Director Center for Democracy & Technology

Yeah, no, no, no, I think you can go ahead.

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

So, I was just arguing that it is technically feasible, as deployed at least in one national scale service, to manage accurate matching with hundreds of millions of people in the database. And we heard that in the testimony from Surescripts when we did the patient matching hearing two years ago, whenever that was.

W

Yeah.

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

And there are advances in matching technology since that testimony that make it even easier to do it. So, I think if we want to have an argument about false positive matches, that's an important argument, but I don't think that has anything to do with directed query, per se.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Yeah. I think we have to – we have to just – that's what I was trying to say to this is, is it policy problem to do a national query, just to get away from arguments that might be supporting a decision that were based on current technology or assumed implementation or something like that. I, so, one of the – we've heard a situation now that Leslie described, that pointed to a disadvantage of national services, which is, stalking. It's not clear to me that it actually makes a lot of difference, I suppose there are some circumstances – in general – one of the things that I understood from Judy was that the patient consent is asked at the time the search is performed by the person who's performing the search, it's not saved somewhere in a database of consents. Was that correct Judy or ...?

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

I don't think that's exactly right. Let me check on it, and I'll get back to you in a sec.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

All right. Okay. I mean, bottom line is that if someone is being stalked, then I would assume that they would withdraw their consent for aggregation services.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Right.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

So, I'm not sure how much that – I'm just trying to get what are the dangers inherent in national search versus what are the benefits. The benefits are, well, what are the benefits?

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

Well the one benefit is that patients frequently remember where their care was, sometimes they're unconscious and can't provide it, and in fact, they might be in Florida when that happens. I mean, there's certainly a – you're increasing the sensitivity, the question is, can you do it without cost of specificity? And I think the answer is yes, you can, there are services that demonstrate that.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

This is Judy again, to answer your question. What happens is that the patient is asked do you want me to search for your record? So, that's what happened to me when I went through it, you're asked if they want you to search for the records, and then the place that you're giving – who is the source of your record, consent over a consent form for me to sign, or enter into my chart or different ways to do it, that authorizes that.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

So, in all cases, the requesting institution has the patient there and is relying on asking the patient directly?

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Oh, well, then it can be stored as to how I want to do that in the future.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Oh, I see. Okay. All right.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

I – and I can do that ahead of time too, which is a good idea. So I might say ahead of time, yes I want my records shared.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

All right.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

And then the other thing is that, we have a lot of snowbirds here, so there are – one of our patients might go to Florida and it doesn't matter, the geography is irrelevant because it's simply a phone number.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Right.

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

Well, I certainly agree that the geography ought to be irrelevant.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

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

And that you want to minimize the – I mean, if you want to address the matching issue, address it by addressing the matching issue rather than by some arbitrary constraint on where the patient happens to be when they need care.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Right, right, and in addition to having made a policy recommendation that was accepted by the Policy Committee on giving patients choice about being in an aggregator service. And also giving, calling on the ability to – recommending that patients have the ability to have an audit report, or some sort of log of who has queried your records and what was released and that's an important aspect of sort of thinking through the stalking scenario that Leslie put on the table. Not that, I mean, that it's actually prevented in the first place the versus having to chase it down after the fact, but certainly, that's another transparency piece that's sort of added to patient comfort level here. I have to admit that I'm struggling with thinking through like what the policy gains would be of creating sort of an arbitrary set of limitations that over – that outweigh the benefits of sort of being able to query. Assuming all of the other factors are in place, like the provider does have a direct treatment relationship, which is the scenario that we're talking about, it's – I'm struggling too with thinking that we would need to put any additional limitations on this from a policy standpoint, given what we've already said.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, this is Paul. I mean I'm listening to everybody and I haven't heard anybody advocate for a reason why we need to create a policy. It sounds like what Judy and Epic has done is a reasonable thing. And it also strikes me that creating a policy around this might be a little bit dangerous with the current sort of initial stage that information exchange is in, because we might accidentally choke off something, that for reasons that we don't understand right now, might be very useful to do in six months or a year. So I don't hear anybody saying yeah, we need a policy on this. I mean, am I hearing it wrong, is there somebody who thinks we should?

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

I – this is David. You've got my vote.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah. I mean I think we need to wordsmith it as, we didn't see a need for a policy that would somehow limit nationwide queries, given that there could be benefits to them. And that we have already recommended a number of protections that would be designed to curb any potential, if it exists out there, for people to misuse a nationwide search capability.

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

This is John Houston, I would agree with that approach.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Well, that's good.

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

Wow.

Paul Egerman – Businessman/Software Entrepreneur

It has the secondary benefit which is that when we presented in front of the Policy Committee a week or so ago, Deven, we were actually completed.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

We were completed.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, because there's nothing else for them to approve.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Oh, that's true. We just have to report that we resolved this.

Paul Egerman – Businessman/Software Entrepreneur

That's right.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

We have no recommendations pertinent to this, other than policy not needed.

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

Well no, I think we do have a recommendation. I think the way you couched it Deven, it speaks as a recommendation actually.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah no, I agree. I agree.

Paul Egerman – Businessman/Software Entrepreneur

There was valuable information there, I agree John.

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

Yeah, I thought the patient choice, transparency services, direct treatment relationship, those all added together makes a pretty strong policy actually.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah. Yup. And just reiterating that in the context of this particular question as a reason why we don't think that there needs to be any sort of limitations that – beyond what we've already – the parameters we've already laid down. So, all right. Well we'll work that up. I think it sounds like we have consensus, we'll wordsmith it, work it up for you to review, but we are about a half an hour ahead of schedule. For some reason Paul and I both thought this one would take a longer amount of time, but it's good that it didn't, and we can move on to the next topic, assuming that Kathryn's ready. Are you on?

Kathryn Marchesini, JD – Office of the National Coordinator

I'm here Deven. I'm here.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

All right, perfect. All right, so what we're moving into now is, doing our part to contribute to Meaningful Use Stage 3 recommendations. As the Tiger Team may recall, there was a Request for Comment that was put out a few months ago, on some proposed criteria for Meaningful Use Stage 3. Many of them were framed as objectives, meaningful use objectives, but some of them were actually framed in terms of technical capabilities. And the ones that are in...that fall into the privacy and security issue bucket, we have been asked to review them and to provide feedback on them, as the Policy Committee continues to consider its recommendations for Meaningful Use Stage 3. And so what we were going to do next, we have Kathryn Marchesini from ONC, from Joy Pritts' team, do an overview. She gave the same overview to the Policy Committee, but there will be a number of you who haven't seen it and a number of the rest of us who did see it who could stand a refresher. It's a high-level summary of the comments that came in, but as I mentioned in the beginning of the call, you also received copies in several files, of the excerpts from the comments that were submitted, again, that are pertinent to the issues that we will explore. And those are really for those of you who really want to understand what those comments were in more detail. We will not be going through those; they are for your background and self-education purposes. Before we hand the call over to Kathryn, Paul was there anything you wanted to add about this.

Paul Egerman – Businessman/Software Entrepreneur

No, I think you did a good summary.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay. Anybody else have any questions before we turn it over to Kathryn to go over the summary slides? Okay Kathryn, you're up.

Kathryn Marchesini, JD – Office of the National Coordinator

Great. Thank you Deven and Paul. For each of the nine privacy and security related questions that were posed in Meaningful Use Stage 3, the Request for Comment that was issued in November 2012, I'll mention a topic area of the question and then briefly touch on high level themes of the actual public comments that were sent and submitted for the specific question. Next slide please.

The first privacy and security question focused on how the recent HIT Policy Committee provider authentication recommendation, which actually originated from the Privacy & Security Tiger Team, how they could be reconciled with the National Strategy for Trusted Identities in Cyberspace, commonly referred to as NSTIC, the approach to identification. Of the actual 41 comments, many of them stated that the NSTIC model could be adopted in health care and strong identity proofing and multifactor authentication should be required for Meaningful Use Stage 3, and to leverage existing standards. You can see examples of some of the existing standard sources that are listed on the slide. Other commenters do want multifactor authentication to be required for MU Stage 3 – excuse me, they do not want it to be required because of the unrealistic deadlines, burden and cost, and it not being a core competency of the EHR itself. Next slide please.

The Request for Comment also asked a related question about how these two-factor authentication recommendations could be tested in certification criteria. Of the 26 comments received, some suggested approaches to testing included developing a checklist to verify that the system set-up. Another approach included requiring attestation to having architecture that supports third-party authentication and require actually a demonstration. A third approach focused on developing a model protocol for self-testing and an iterative and phased testing program. Commenters noted that existing standards and guidance could be the basis of test procedures, and you can see on the slide it highlights some existing standards that were mentioned. One commenter did note that in general the domain is not mature enough for certification criteria for testing authentication. Next slide please.

The last question dealing with authentication focuses on whether there should be certification of an EHR as a stand-alone entity and/or an EHR with a third-party authentication service provider. Many of the 30 commenters supported both approaches for certification, while several suggested permitting the certification of the EHR and third party authentication service provider independently of each other. Commenters also provided suggestions around certification in this area including handling third party dependencies in a way that is similar to those in other sectors, implementing NSTIC in lieu of requiring certification and leveraging NSTIC accreditation authority to assist with certification and using external labs with the capability and experience in testing in this area.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Can I ask – yeah, Kathryn, hold on a second. Can I ask the person, someone who's background noise, to please mute.

Kathryn Marchesini, JD – Office of the National Coordinator

Thanks Deven.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Thank you.

Kathryn Marchesini, JD – Office of the National Coordinator

In slide 10, next slide please. In slide 10, in looking at building on existing privacy and security related meaningful use requirements, the RFC requested identification of security risk issues to address in MU3 and feedback on requiring whether providers should attest to implementing HIPAA security rule provisions regarding workforce, outreach and training and sending periodic security reminders. And regarding to the attestation for workforce security outreach and training, some comments support

requiring attestation regarding workforce outreach. They cited the importance of workforce in keeping the overall patient information secure. Many comments were against this attestation.

Commenters most frequently noted it would be either burdensome or duplicative of the HIPAA security rule. Other comments are neutral toward the attestation requirement, but mentioned that it would need to – in general, it would support HIPAA security rule provision, so there was no specific reference to support or objection to an attestation. Commenters identified other security areas to emphasize in our Meaningful Use Stage 3, which you can see listed on the slide. Some of them included emphasis on access controls, encryption, as well as backup and recovery and storage of protected health information. Also, some commenters requested the need for more HIPAA security rule guidance and general education for providers. Next slide please.

And the fifth privacy and security question posed in the RFC, there is the request for feedback on a prescribed certification standard for audit logs. The majority of commenters noted that the prescribed ASTM standard is feasible to use for certification of the compliance of an electronic health record. Other comments questioned whether or not there should even be a certification standard covering this area. And some of the reasons that were cited include waiting until the promulgation of the final HIPAA Accounting of Disclosures Rule, suggested conducting additional feasibility studies and research before mandating a standard in this specific area. Some commenters generally noted that the question...the RFC question conflates audit logs, which is focusing more on electronic capture, with the accounting of disclosures, which dealt more with report production. Next slide please.

In response to the RFC question about whether or not it's appropriate to require attestation that audit logs are created and maintained for a specific period of time, many commenters suggested until the promulgation of the final HIPAA Accounting Disclosures Rule before specifying any attestation or an audit log requirement. Many commenters supported adding this audit log attestation requirement and identified other points to consider when developing the requirement, and you can see some of these listed on the slide. Some of these do include relying on existing NIST standards or other federal or state regulation, specifying the specific period of time and identifying the minimum data set. Other comments suggest expanding the attestation to all requirements in the HIPAA Privacy and Security Rule. Next slide.

The majority of commenters are neutral toward attestation in this area. This means that the comment did not especially agree or disagree with adding the attestation requirement. Various reasons were cited including wait on the final HIPAA Accounting of Disclosure Rule and have mentioned completing feasibility studies before making a decision. Others disagreed with adding the attestation requirement in general. The reasons that were cited were administrative burden, there's not an improvement to the security and the audit log is only a functionality of the EHR and it's not for provider attestation. Next slide please.

Many commenters generally noted that there is not a dominant or mature existing standard to meet the stated need for an audit log files of EHRs that were posed in question 7. Most commenters support a need for a standard format requirement in this area. Others are neutral toward a standard format or they say that the adoption of such a standard would need to overcome the challenge of the variability of details captured by existing systems. Some commenters disagree with the need for a standard format citing that it would be a burden for health care organizations and vendors, and others noted only a minimum data set or elements should be defined in MU Stage 3. Also some commenters stated that there's not a need for an MU based standard related to the accounting of disclosures. Next slide please.

A related question about audit log file format specification received 37 comments in which respondents mentioned many existing specifications that could be considered for audit log purposes including those listed on the slide. Some comments noticed that while there may be existing specification or standard, none of them are widely adopted, although there have been multiple attempts to develop a standard audit log format. And while other commenters opposed the addition of any new meaningful use requirement based on the proposed HIPAA Accounting of Disclosures Rule. Next slide please.

The last privacy and security related question focuses on the technical capabilities of patient consent and consent management. The RFC put forth three questions in this area. In regard to how EHRs and HIEs can manage information that requires patient consent, many commenters indicated support for a metadata tagging approach to enable this type of consent. Several noted that data segmentation capabilities currently exist and have been demonstrated, you can see some examples on the slide. However, other commenters stressed that segmentation capabilities required to enable this type of consent management are not currently existent in the vendor market. Commenters provided alternatives including focusing on identifying and punishing inappropriate use of data, while other commented that an easier way to accomplish consent management is to give patients control of their data via a personal health record. Next slide please.

In response to the question regarding the capacity of the EHR infrastructure to record consent, a number of the comments support the idea of creating or promoting standards to improve the capacity of the EHR infrastructure to accomplish this. Also a number of comments specifically support creating standardized fields for specially protected health information. Several comments recommended that all certified EHRs be able to manage patient consent and control re-disclosure. Also, some comments recommend that an EHR system be able to modify the actual consent over time. In response to I guess the last question, as to whether there are existing standards that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIEs, responders noted that the efforts of the Standards & Interoperability framework, Data Segmentation for Privacy Initiative that's looking at the ability to convey whether the individual has consented or not. They also reference HL7 confidentiality and sensitivity code sets, the VA/SAMHSA pilot in this area and work developed by the eHI and being done in some of the states and HIEs.

So, that concludes a snapshot of the comments that were received from the public regarding privacy and security questions in the RFC. If you're interested, I know Deven had mentioned if you want to do a deep dive, that you should – the Tiger Team members should have received the comment summaries and links to the actual public comments as part of today's meeting materials.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay. Terrific Kathryn, that's very helpful. Does anybody have any questions for Kathryn before I turn it over to Paul for the discussion part? Okay. Kathryn thank you very much for going through all of that with us. It's almost like you don't – try to remember that we formulated some of those questions way back when, not all of them, but some of them. Nonetheless, they all sort of fall into the privacy and security category. Whether or not they're all sort of related to policy or whether some of them are more technical in nature is another question. So Paul, are you ready to drive the bus?

Paul Egerman – Businessman/Software Entrepreneur

Sure. And, I expect you to be around for just a few more minutes Deven.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, oh yeah.

Paul Egerman – Businessman/Software Entrepreneur

But again, to reiterate, this presentation – Kathryn, thank you very much for the terrific presentation in summary of what are also extremely important comments. And the purpose of these comments and feedback is to help us with our work, so that we can gain more information and understand what we should be doing. And what we probably need to do in terms of discussing these comments is to first ask people if they have some general impressions from the feedback. And then the second, to look at these comments and to see if there's some of the questions and issues here that are really issues that belong to the Standards Committee, that are perhaps some of the stuff about the audit logs are not issues that we need to address. And then to see what are the issues that are here that we need to address that we have not yet addressed. So that's the way I'm looking at that, I don't know if that's correct Deven, but that's the way I'm looking at the situation.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah. No, I think that's absolutely correct. I think the first thing we have to do is figure out whether...which of these in fact are sort of policy questions that we need to deal with and which of them are more technical matters that the Standards Committee and the Privacy & Security working group of the

Standards Committee should be tackling. And then the second thing I think, the other item to keep in mind is that these questions on the RFC went out well before we had finished our work on query, specifically around sort of the technical capabilities around sort of dealing with consent issues and communicating information about when a patient's consent is required and what that consent needs to look like. And so we did include in background to these slides, just a reminder of sort of where we landed on those questions.

So there for example, and also on the issue of logging, at least for query purposes. So we're reminded on slide 20 of sort of where we landed on technical capabilities for logging queries and responses. Similarly, beginning on slide 22, we have sort of what we said from a technical standpoint about communicating applicable consent needs or requirements and being able to maintain a record of that and sort of passing information back and forth between the relevant parties to a query. And all of that we landed on sort of well before the RFC was issued, and so certainly what we've already said on the topic would be relevant. But...and I think you're right Paul that the threshold discussion is which ones of these are ours and which ones of these are theirs. And which ones might we have to work on together; I suppose that's another third.

Paul Egerman – Businessman/Software Entrepreneur

And so, we would like to start this, which of these are theirs? Let's start and see if we can shorten the list a little bit, in terms of what are the issues here that don't strike people as policy issues, are issues for standards or for certification testing or something else? Does anybody have any comments on that?

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

So this is David. I think obviously the ones about formats of logging files, the question around ATNA and others would be Standards Committee material straight up. Some of the other ones might not be so clear, but...

Paul Egerman – Businessman/Software Entrepreneur

So that's – I'm just looking at this again, but, that's like number 5, the certification standard for audit logs.

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

Yeah. It seems to me that we actually, we rendered an opinion at the Privacy & Security team, Dixie's workgroup did render an opinion on that back in Stage 1, although it may be worth revisiting for Stage 3.

Paul Egerman – Businessman/Software Entrepreneur

There are a number of questions about the logs here.

Kathryn Marchesini, JD – Office of the National Coordinator

Yeah, there are. There's like three or four of them, all in a row.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, there's numbers, so number 5 is like that, number 7 is like that.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

This is Wes. I would support that – I would suggest that everything from 2 forward, through the PSTT numbers is certainly theirs. Number 1 ...

Paul Egerman – Businessman/Software Entrepreneur

Okay.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

This gets into an awful lot of technical evaluation about the feasibility; ultimately I think there are some policy issues in there though.

Paul Egerman – Businessman/Software Entrepreneur

Okay, so you're saying the PSTT ones, you're saying the first one, starts there is a policy issue, but all of the others strike you as like standards issues? Do I have that right?

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Well, number 1 strikes me as a policy issue buried in a whole bunch of technology issues.

Paul Egerman – Businessman/Software Entrepreneur

Okay.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

The others are all just technology issues.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I, well, except I think I would argue, hold on, I know I've got control of the slides here, I think the only other – I would agree with you Wes, save one exception. And that's the PSTT 04, which I just flipped to, it's slide number 10, for people who are not online. And this is related to, keeping in mind that we've had recommendations going to CMS and ONC related to a meaningful use objective that shines a spotlight on a HIPAA Security Rule issue that we want people to specifically attest to having addressed. So in Stage 1 it was the risk assessment, doing the risk assessment and then in Stage 2 it was reviewing risk assessment and attesting to addressing encryption of data at rest. And so I think I would argue that stage, that this one is about whether there are – are one or more or none other topics already addressed by the Security Rule, but that we want to use the Meaningful Use Program to shine a spotlight on. So, I think that's ...

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Yeah, I agree. I zipped through that one too fast.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

No, that's okay. I mean, it's been a while since folks have looked at this, but aside from 1 and 4, I'm sort of in agreement with you that I think that they – that the rest of them are more technical in nature. And one option that we have is to sort of ask the Privacy & Security working group to take a look at them and bounce back to us any policy issues they think are hidden in there that we didn't see.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Deven, what about – identify a minimum data set on 06? I'm not sure what it means by requirements for identifying a minimum data set, but the minimum data set itself is kind of a policy decision.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, I suspect that's related to what would be the minimum amount of data that would be collected in an audit log, and ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Oh, okay. All right.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Then I'm okay with it.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, and this is Paul. The things I have from that commentary, I did read that comment, it was, if I remember it correctly, that individual felt that there really shouldn't be audit logs and specifications for that, but you could put forward like the minimum data that one should retain, in an audit log. Or one should record ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

So are you saying that that is – if information is brought over, some of it should not be retained?

Paul Egerman – Businessman/Software Entrepreneur

No, that's not what I'm saying. In other words, I'll do my best to express what I had read.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Well what should be retained?

Paul Egerman – Businessman/Software Entrepreneur

What I had read in the comments, where somebody said, you can't really come forward with like a specification for what's going to be audited, but you could possibly start with what is the amount of information that you should have in an audit log was the suggestion. And so that's – that was the issue

that Deven was raising as to whether or not that's a policy issue for us. And I don't whether or not it is or if that's something that standards has to deal with.

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

I think – this is David – the degree to which you might make audit log format a policy issue would be if you felt there was enough policy value in having a standard format to facilitate detection of abuse or fraud or inappropriate disclosure by making it easier to pool sources together, since the audit logs belong with the actual source systems, the activity may be spread over many different systems. So I think the original intent of having a standard was to make it easier to merge them together. And you could argue that that's really a policy decision and the technologist would say, yeah, tell us if that's important enough or not.

Paul Egerman – Businessman/Software Entrepreneur

Yeah but see – this is Paul again. Your comment is a good one David, because in effect what you're saying, we're doing is just speculating why we would be interested in this.

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

Right, right. I'm just trying to ...

Paul Egerman – Businessman/Software Entrepreneur

But the real issue is ...

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

... explain why ...

Paul Egerman – Businessman/Software Entrepreneur

Yeah, then that could be one reason, I suppose.

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

I mean, when we've had this discussion in the past, about some of these audit formats, like ATNA, for example, which is a fairly non-trivial format to implement and a lot of vendors have implemented something that is close to ATNA, it kind of follows the spirit of ATNA, but it's not actually technically ATNA. And the question is, should we go further, should we put the extra effort into being completely consistent and, I think you could argue that that's really a policy, because it's a lot of cost and you have to decide what's the benefit. And the benefit might be that it improves the ability to detect abuse, because it makes it easier to do broader queries across multiple systems that might be working together in a regional network of some kind. On the other hand, it's a lot of work for the vendors and they don't want to do it unless there's a really good reason to do it.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I'm sorry to interrupt, I'm going to have to drop off myself, this is Deven, leaving you in good hands and look forward to picking the conversation when we reconvene. Thank you.

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

We'll miss you.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Thanks. Bye.

Paul Egerman – Businessman/Software Entrepreneur

So, your comments, David, are good ones. So the question I have is, if we go back to what Wes said, which is really to take all the PST things, starting with 2, with one possible exception, but taking anything that relates to like the audit, the audit logs and specifications and sort of like say, that's not our thing. And, I'm trying to understand if I'm hearing you right David, are you saying that well maybe it should be our thing; we should have a discussion as to the value of establishing some policies around these logs?

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

No. I was sort of saying something slightly less powerful. I was just saying that if there were to be a policy question embedded in all that technology, it might be what's the relative value of having a standard log without worrying about which standard. But is it desirable from a policy point of view to have a standard logging format, and would that – do we believe that would facilitate detection of abuse and improve the ability for patients to see what's happening to their data and the like. And I think the answer is, it probably – the degree to which it's more standard, there would be – it would be easier to use the data. The

question is, is it worth it. And I mean, it's partly technical, but the technologist will tell you, we could support a rigid standard, it's just a lot of extra work.

Paul Egerman – Businessman/Software Entrepreneur

Yes. And so, I – and I might put forward the idea, is the value is in detection of abuse rather than talk about audit log formats, we should be talking about detection of abuse.

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

Yes, absolutely, I totally agree. Yeah, we would ...

Paul Egerman – Businessman/Software Entrepreneur

And if that's a policy issue we want to address, then we should address it. And as a byproduct of that relates to audit logs, that's fine. But, that's also, well, it certainly could be a privacy and security issue, so.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

Paul, this is Joy. There's another issue that's related to this that I have not heard discussed yet, but which I heard at a meeting I was attending, which is, it's almost like a – I would classify it as a patient safety issue, I think. I'm not positive of that, but, we – I heard from a number of state's medical board investigators of their difficulty in reviewing when information has been changed in a medical record. And I think that might be related to the logging, I'm not positive.

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

Yeah, this is David – I think it would. What was the issue they were – you said it was a safety issue?

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

Well, they can't tell – yeah, because when they're investigating a doctor to see if they've done, engaged in malpractice or something.

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

I see.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

At least in a paper world, what happens often is not – it doesn't happen often, but in the context of people who are behaving badly it happens, they'll go back and try to cover their tracks by changing the record. And so they're trying to remove these people from practice, but if they can't get their arms around what they're doing, then they can't do their duty.

Paul Egerman – Businessman/Software Entrepreneur

And that's very helpful Joy, because, if I understand the challenge there is sort of like, what did the record look like at any point in time and did the physician see it. So, like what do they know and when did they know it. And, if you constructed your logs in theory like a completely like perfect manner, you'd be able to answer any question like that. In other words, you'd be able to, in theory, be able to roll back to any point in time and see exactly what a record looked like. And in theory you'd be able to say, also anybody who had ever seen it at that point in time, what they saw. That would be like one vision as to how that would work. So I don't know if I'm restating this accurately. And so that's a good explanation for the reason, and so my question is, what should we do as a policy tiger team on the issue of audit logs? Should we be shrugging our shoulders or should we say, well these are important issues, those issues the issue that you just raised Joy, which is interrelated with possibly some, or overlapping is a better way of saying it, possibly overlapping with some of the issues that David raised with fraud and abuse. So, should that be a topic that we discuss and then audit logs then becomes one of the vehicles for resolving that issue.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Paul, this is Wes. The thing that concerns me is that when they get to specifying an audit log, we're specifying a solution for some problems. I am not sure, for example, I know that the CCHIT gold standards for EHRs calling for being able to see every change that had been made in an electronic health record and who made it, and I actually thought that was pretty common among electronic health record systems, although not universal. Without – and that's without having to get a specially authorized sysop to take out and decode the audit log. As far as who looked at the record, that's – I don't know if that's beyond the level of what an audit log can do. It sounds to me like there's some desirable functionality associated with EHRs and their milieu that are important policy issues and we should be looking for those. And then if we can identify those, then we should ask the question, is the audit log the appropriate approach is requiring it be done through a standard audit log an appropriate approach or not. I mean a lot, there are a lot of places that are doing, making do with non-standard audit logs now and getting some fair amount of intelligence out of their systems. There could be no – there can be no doubt that it could be better if the audit logs were standardized.

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

This is John Houston. Can I – just one piece of insider – at UPMC we have an incredibly robust auditing capability. But the question really comes down to, what is the purpose of the audit logs, how much do they – how much depth do we really need to have in them or are we trying – I think part of the problem I continue to see is that people are trying to over-engineer what the purpose of the audit log is. And so, I think that's part of, I think, the discussion we have to have is really, what should it really be and what is its intended purpose and are we trying to do too much with them. Or do people expect to do too much with them and the realization is you don't need to do as much as they expect.

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

Yeah, this is David. That's a good point and the difference between forensics and accounting for disclosures and transparency to patients who want to know what's happening to their data are really probably three very separate things.

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

I agree. I agree. And it's so often the fact that somebody actually looked at the users record is often all you need to explore, once you get to that singular point, the rest is easy, or the investigation is non-technical and becomes an HR, say for the case of inappropriate access.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

This is Judy. Is there some time I could bring up a topic of what I think is a very much better way to keep privacy, to handle privacy than data segmentation.

Paul Egerman – Businessman/Software Entrepreneur

Yes. But not quite right now.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Okay, tell me when.

Paul Egerman – Businessman/Software Entrepreneur

Okay, I just want to make sure that I get through this part of the discussion. But that's certainly an important issue and that does get to some of the MU questions that were at the end. But I want to make sure I wrap up these PSTT questions, which are really about the audit logs. And so, at first I heard, let's just pass this over to Standards Committee, but now I'm sort of hearing, well maybe what we need is to focus less on the formats of the logs and more on an understanding of the various purposes. Because it seems like that was a valuable discussion we just had when people started to say, you know there's forensics, there's disclosure to individuals, that there's some fundamental functions and that perhaps there are some important policy issues there as it relates to patient transparency and also to patient safety. So, I'm starting to think that well gee, maybe we should just approach the issue more from like a functional standpoint and be able to come up with at least some broad policy statements about what is needed in terms of an auditing function, whether or not, how that gets implemented, then we pass it over to Standards Committee. Does that sound like a better approach to these questions? Or does that sound

appropriate?

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

I agree.

Paul Egerman – Businessman/Software Entrepreneur

Pardon me? Okay, I heard one person say I agree, then I heard ...

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

Paul can you hear me?

Paul Egerman – Businessman/Software Entrepreneur

Yes, I can hear you.

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

Oh, okay, the mute button on this phone is confusing, so I wasn't sure if I was muted or not. No, I think that makes sense. I mean, it's a huge issue and to focus in on whether the log should be standard or not when you haven't decided what you're trying to do with those logs might be kind of wasting your breath. Although some of its constrained by the requirements of HIPAA and then some will be constrained by the Accounting for Disclosures Rule, I think there were a couple of comments to that effect that we should wait until that's settled. I don't – has that actually, the final version of that come out? I don't think it has, although I can't keep track.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

No it has not.

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

Okay.

Paul Egerman – Businessman/Software Entrepreneur

And then also, as I look at these questions, within the logs, there does seem to be some issues where we might want to make some statements. In other words, besides the standard format, there are questions about how long you maintain information.

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

Isn't that legally regulated already?

Paul Egerman – Businessman/Software Entrepreneur

I don't know. Yeah – the time logs – is it legally regulated?

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

No I think the law is how long you keep the health information of the patient, I don't know about laws about the audit log.

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

Yeah, that's what I was just about to say, is it – there are rules around the record itself, but maybe not around the log of access.

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

The log of access has to be kept for, I forget, I think it's six years.

M

There are numerous I – HIPAA does define a period of time.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

Well no, HIPAA defines it – well, HIPAA defines a period of time where there's a requirement to document.

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

Well yeah, but that means you have to keep the access logs for that period of time, I don't know how you could document it otherwise.

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

It would be sort of pointless to keep the audit log longer than the actual record; I guess you could argue keeping it less.

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

No, no, no, I think the point is you have to be able to do an accounting for a certain period of time, I think it's what 6 years or ...?

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

Yeah, no, that was my memory as well, that it was already specified. Maybe it's in the interim final.

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

But for internal access associated with treatment is what, three years I guess then, right? I think there's diff, a varying length you had to keep these logs, but nonetheless, there is a period of time prescribed.

Paul Egerman – Businessman/Software Entrepreneur

So, you answer this question about the length of time and whether or not that's a policy question. I'm unclear as to the answer, other than I think what we'll check with our HIPAA experts to decide whether or not that's a topic that we also need to discuss.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Yeah. See, I think that we have sort of two unattractive options here, but there the best we've got. One is to really, to wait for the Accounting for Disclosures Rule because if it follows the proposed rule, it really creates a bunch of requirements around –implies a bunch of requirements for audit that were not at all implicit in any prior regulation or the law, because they took a fairly creative approach in creating the regulation. Most of what's been required for accounting for disclosures in the past has been accounting for disclosures external to the organization, and I don't think EHR audit logs have much to do with that, to be honest. They might be one aspect, but ..

Paul Egerman – Businessman/Software Entrepreneur

Okay.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

So I guess the problem I have with this is that it's going to be hard to discuss it until we know the direction of that rule, but as far as I know, the published information about what rules are, like what stages they're in, there's nothing published about what stage that rule is in.

David Holtzman, JD, CIPP/G – Officer for Civil Rights

Hi, it's David Holtzman with OCR; perhaps I can help a little bit with this. So we do not have a timeline in which we're going to have a final rule out. We are looking at it, and it is on our work plan and we've been looking at the comments and so, I don't think we're going to be able to provide you any relief in the short term as to a direction to send you in.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Yeah.

David Holtzman, JD, CIPP/G – Officer for Civil Rights

So, I think Joy and Deven will be able to assist you in that and...but you're not going to get a resolution to the question probably in time for when you're going to need your – need to make your recommendations.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Yeah, that's what I thought.

Paul Egerman – Businessman/Software Entrepreneur

Well, and I thank you for that comment also. It's extremely helpful.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Useful, yeah.

Paul Egerman – Businessman/Software Entrepreneur

And it's a wonderful thing to have you participate in this call, so I appreciate OCR's help.

David Holtzman, JD, CIPP/G – Officer for Civil Rights

Well, I get as much out of it as you guys get from our comments.

Paul Egerman – Businessman/Software Entrepreneur

Well that's good to learn and to hear.

David Holtzman, JD, CIPP/G – Officer for Civil Rights

These conversations are very helpful.

Paul Egerman – Businessman/Software Entrepreneur

So, as I look at the whole issue of audit logs, it's still an issue of we should be talking about it in the context of functionally what we're trying to accomplish with them, in terms of some of these things like patient safety, accounting for disclosures, forensics and our policy view should sort of like derive from that. And I do understand what Wes is saying about the challenges about the rule on – the status of the rulemaking on Accounting for Disclosures. So, why don't we also just move on, to make sure we also talk about the other questions that were raised. Because what we're trying to do in this part of the discussion is not solve these things, it's try to get some sense as to how we're going to address these topics and then we're going to try to put together some like agenda and schedule for you.

So we also have these MU4 questions on patient consent. And so, it seems to me there's a lot of information here. Now some of this we may have already addressed, and a lot of it deals with this issue that Judy was asking about, relating to data segmentation. And Judy, you said you have an idea contrary as to how ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Yeah. Right. Well first of all I want say why I don't think data segmentation is good. I think one thing technically it is – has not been, as you have in your notes there, has not been used by anyone in any large numbers to show that indeed it works successfully. And secondly, I think it can mislead the patient because a patient can believe certain things are hidden and they're not. In other words, people might be able to figure out from the labs that are ordered what wasn't released in the lab results or from the care team, who's taking care of the patient, stuff like that. So I think it's a very inacc – inexact and inaccurate approach to do it with data segmentation. What I recommend is that we allow patients who request it, to create their own CCD document basically, so they can put down anything they want. So if to them the most private thing that they don't want shared is removing the big wart in their nose, that's their choice, they can do that. And they can look through it and make sure it is comfortable for them that gets released. It is identified as the patient provided document and therefore everything on it is something they're comfortable and that rule that says there won't be any surprises, is maintained.

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

The only harm with that ...

Paul Egerman – Businessman/Software Entrepreneur

(Indiscernible)

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

This is John Houston. The only problem with that is I've heard too many physicians say that those become medical fictions that they don't even want to see.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Well the other medical fiction is that you have something with data segmentation where indeed it's not the same either.

Paul Egerman – Businessman/Software Entrepreneur

And so here's – let me interrupt this discussion John. This is an important topic and I'm looking at the clock and we have 10 minutes left in this call.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

My gut feeling is we're not going to resolve it in 10 minutes.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Right.

Paul Egerman – Businessman/Software Entrepreneur

Just a guess. But ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

But there's ...

Paul Egerman – Businessman/Software Entrepreneur

There's some privacy and segmentation issues are at the core of these comments, and what you just said, Judy, is consistent with what some of the commenters said.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Um hmm.

Paul Egerman – Businessman/Software Entrepreneur

Like some of the commenters said, well gee, there's going to be a problem if you withhold information. The comments on this, I know that Deven said that you don't have to read the individual comments, but I actually found, there's one document that we sent out that had them all sort of put together on these MU4 comments. And I thought that was very, it's like 20 pages long, it's a lot of reading, but I thought it was really very valuable to read. Because you get some comments that are similar to what you're saying Judy, comments from clinicians who are concerned, but there are also comments – a lot of interesting comments about substance abuse and some of the challenges there, and how some of the rules and laws are set up prior to health information exchange. So I think that that's valuable information, but I just have a suspicion, although I'm not quite sure I know how to organize the discussion yet, but we do need a lot more discussion on ...

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

A lot of these topics to get some understanding and consensus and as to how – as to what we should be doing.

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

This is David. We – Paul, we had a presentation from the data segmentation group on the last Privacy & Security call for the Standards Committee, Dixie's workgroup, and it took almost the entire call just for them to explain their model and then ...

Paul Egerman – Businessman/Software Entrepreneur

... the model, I think I was on that call with.

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

Yeah, you were that's right; it was a joint call, good, good memory. So I'm just saying this is a really intensely complicated and I share Judy's perspective that it's just really hard to see how to implement it in a way that won't have profound impact on provider productivity. I don't know what that means, but we're not there yet with what's been proposed. It's a challenge.

Paul Egerman – Businessman/Software Entrepreneur

Well, and that was one of my takeaways from the meeting, was when I saw that you, David and Judy, seemed to be agreeing, coming from very different directions on some of the issues, made me think that we've got some interesting challenges that we need to address. So what we'll have to do here is, we'll work with Deven and Joy and see what we can do to structure some additional discussion. The hard part is, is we don't want to repeat things that we've already done, and we also don't want – we want to make sure that we're guided by existing law, I mean, some of these things you just have to do. But there is – I

would encourage people to read through those comments that are called the MU4 comments, in fact, I'll see if we can send them out that one document out again so people could go through that, really very thoughtful comments. But I think what we've done today is we've accomplished what we wanted to do, we wanted to finish up our query discussion, we wanted to get briefed on the responses to the RFC, and we wanted to have this discussion where we had some feedback from the group at least on the topics on the comments, so that was all helpful. And so I'm wondering now if it would be a good time, MacKenzie, to see if we have any public comments.

Public Comment

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator for Health Information Technology

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

Rebecca Armendariz – Altarum Institute

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

Paul Egerman – Businessman/Software Entrepreneur

Great. Well thank you and thank you to all the members of the Tiger Team for another excellent discussion.

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

Thanks.

Paul Egerman – Businessman/Software Entrepreneur

Bye, bye.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

Bye.

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

Bye.