

**HIT Policy Committee
Privacy & Security Tiger Team
Transcript
June 17, 2013**

Presentation

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – 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 on 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. Deven McGraw?

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

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Deven. Paul Egberman?

Paul Egberman – Businessman/Software Entrepreneur

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Paul. Dixie Baker?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

I'm here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Dixie. Judy Faulkner?

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

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Judy. Leslie Francis?

Leslie Francis, JD, PhD – University of Utah College of Law

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Leslie. Gayle Harrell? John Houston?

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

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks John. David McCallie?

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

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks David. Wes Rishel?

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

Here.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Wes. Micky Tripathi? Kitt Winter? And any ONC staff members on the line, if you could identify yourself please.

Kathryn Marchesini, JD – Policy Analyst – Office of the National Coordinator

Kathryn Marchesini.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Kathryn.

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

David Holtzman, Office of Civil Rights.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks David. So, I will turn the agenda back to you Deven.

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

All right, terrific. Thank you very much. Thanks to the members of the Tiger Team for coming on to the call today and thanks also to members of the public who may be listening in. We're going to spend time on this call, at least the first part of the call, sharing with you the status of the virtual hearing that we have planned on the non-targeted query issue. This hearing actually will take place next week and we're quite ready for it. We're still hearing from some of the invitees, as we'll talk about, but we are certainly feeling like this is going to turn out to be one of our – a very good and informative exercise for us. I'm kind of excited about it.

Then after we sort of share sort of what the status of the hearing is, we didn't have any additional substantive material teed up and since we had the space on calendars, I thought we could go ahead and talk about the issues relating to security risk assessments for Meaningful Use Stage 3. And whether there might be other options for helping to ensure that people are actually doing these as part of meaningful use, maybe something beyond attestation. And we had a number of people who volunteered to be in a subgroup for this, so we're going to go ahead and sort of have that subgroup meeting during this regular Tiger Team call, since we already have the time carved off. And essentially what we'll do is allow those of you who would prefer not to take part in the subgroup discussions and just wait to hear the outcome of those discussions, you can actually hang up and go about your day. But for those of you who expressed an interest in, and would like to be on the subgroup, or even if you initially didn't say you wanted to be on the subgroup, but as long as we've got it scheduled during a regular Tiger Team call you can join in on it, then of course you are welcome to stay.

Of course, if we end up talking about the hearing for the 90 minutes we have scheduled for this Tiger Team call, then we'll have to pick another time for the subgroup hearing. But I think we're in very good shape on the hearing and I'm hoping we can at least start to deal with the subgroup issue on this call today. So, I actually just covered this slide. All right, does anybody have any questions about the agenda and what we're planning to do before we move forward?

All right, terrific. So once again, we have the virtual hearing, which will take place next Monday from 1 to 4 p.m. Eastern time, so a little bit of a break for our West Coast members, because they won't have to get up at the crack of dawn to do this, which is nice. The material I'm about to summarize on these slides is – sort of articulates the purpose and scope of the hearing so that it's abundantly clear to the people that we are asking to present to us, and also abundantly clear to members of the public who want to join us. It is language that you've seen before by email and that we had previously asked you for comment on, we didn't get a lot of feedback on it, but we did get some helpful feedback from folks. So, wordsmithing this language is – it's already language that's gone out to the folks who have been invited and so we definitely don't want to spend time on this call wordsmithing the language.

But certainly to the extent that anybody wants to sort of talk about an issue that isn't adequately covered, to make sure that it's something that gets surfaced in the question and answer period. We do have slides that provide status on the people who have been asked to present to us and what we've heard from them so far. We have a good list, I think. We're trying to sort of have two panels, essentially, even though there's not – the panels are not divided so much by an expectation that there will be people speaking to different topics, but asked everybody to address the same topics. But just to chunk up the hearing a little bit, so that there are – there's time for questions from the Tiger Team kind of interspersed with the presentations that we expect to hear.

So going back to the overall purpose of what we're trying to do here. We are trying to sort of understand the sorts of policies that are deployed in order to ensure that a non-targeted query, as opposed to the targeted query for which we've already had recommendations adopted by the Policy Committee, ensuring that a non-targeted query for a patient record is appropriate, legal and authorized. And we really are in this hearing focusing on policies and not security methodologies or even identity management issues. We have a slide that sort of describes sort of some of what we're talking about when we say policies governing non-targeted query. For example, it might include limitations on who can conduct a query, the purposes for which it can be conducted, maybe they're geographic or other limits in parameters, intended to help assure proper access and demonstrate that the requestor's authorized to access those records.

We are particularly interested in hearing about environments where there are some limitations that have been adopted to place limits on query. But again, we're also interested in hearing of instances where, in fact, there policies may have been considered but ultimately weren't adopted. And we want to learn about sort of what the thought processes were. This is the lie to be more specific about it, why did they adopt the policies or why did they decide not to adopt policies. Clearly we want to make clear that – or, it's clear to us, but we want to make it clear to the public and to the people who are making presentations for us, that we're focused on queries between disparate entities, so not queries within an organization or an OHCA or an integrated delivery network. And we also, of course, want to make clear what we mean when we say non-targeted query, which is a circumstance where the patients other providers are not known in advance. And so that means you're looking of patient's record using information about a patient, and this is what makes it distinct from the targeted query models that we used before. It involves using an aggregator service and we have some examples of what these are commonly called, although this is not certainly an exclusive list. And on the issue of query generally, we've been focused on query for direct treatment purposes, but since we're having this hearing, it will be – we have an opportunity to determine whether the entities that we are asking to make presentations to us have deployed non-targeted query models for other purposes as well. Because arguably, limiting non-targeted query for treatment purposes is itself a policy limitation.

And here is a visual for folks to have – get a better understanding of the concept of non-targeted query from looking at a picture versus from seeing it spelled out in language. Being a lawyer, I'm exactly the opposite, maybe it's because I'm a lawyer who was bad at math or art, but this is a conceptual picture for folks that I think certainly captures again the concept of what we are talking about with respect to a non-targeted query. And then we have a proposed set of questions, and again, this is all material that's going out and has gone out to entities that we are seeking to present to us. And again, these are questions that we had previously circulated to you, we talked about them in one of our previous Tiger Team calls, we got some feedback there. We asked for additional feedback by email and then needed to get these out to entities testifying for us.

The entities that are being asked to testify have been asked to present information on these specific questions. And there are a number of questions, and so we are giving people the option of answering the questions that are the most relevant to the particular model of non-targeted query that they are deploying. And we will have an opportunity, obviously, to ask questions if we sort of feel like there are questions either in this proposed list or that occur to us as we're listening, that they maybe don't address with their verbal testimony. We did not ask or require people – we did not require people to submit written testimony to us, we feel like people are doing us a favor to take time out of their busy schedules to provide us with this information and making it as easy as we possibly can for them was certainly a goal. Although of course, we have invited them to submit any materials that they would like to in writing, they can answer some or all of these questions in writing if they want to, and they can also submit any additional materials about their particular exchange model, if they think it would be helpful.

So we're not expecting, necessarily, to get a lot of written materials in ahead of time, we are going to try extremely hard to have people focus on policies related to non-targeted query and that's why we've been very specific about a set of proposed questions. And are being very clear when we're asking people, that these are the types of questions that we would hope that they would use their time to answer. We're going with the typical sort of 5-minute limit on verbal presentations, but we're building in plenty of time for questions. So, on the slide are the questions that you all helped us to shape, how they operationalize non-targeted queries? How long has this been going on and how many patients are involved? Do you have an inherent scope limitation such as geography in the case of a lot of state HIEs? What other additional limits have you placed on query? What roles do patients have in limiting query and other circumstances under which patient preferences are overridden, which can be common in emergency circumstances, for example? And how does that process work and have there been any problems? How do patients exercise meaningful choice about whether their records are part of the aggregator service, and does this extend to the – does this choice extend to the release of the data, or does that then require additional consent? How do they address the exchange of sensitive information? What information is actually returned to a requestor as the result of a non-targeted query? And if in fact, sensitive information is involved, is there a difference in what is returned when that kind of information is involved? In what environment and for what providers have these non-targeted queries proven to be the most effective, and if they have metrics on that, that would be amazing. And have they experienced any challenge or problems with their particular approach? And what adjustments do they think – do they have plans for, if any? And then there's this general question that sort of asks them about whether having widely applicable policy, such as what we might propose to the Policy Committee and ask to be adopted, would that be helpful and if so, what would those policies look like.

One of the comments that we did get back from the Tiger Team, thank you David McCallie, was that even though we expressed an interest in knowing the lie behind these policies. We actually don't have it as a – but at the end of the day, since we already had 11 questions teed up for people and we're asking them to try to use five minutes in order to address as many of them as they can. We decided that the why behind these policies might be a better question of us to ask them during the Q&A period especially when we have a little more information about exactly what policies they have deployed in non-targeted query.

Here I'll just show you the sort of list of HIEs that have been invited, and we have a number of them that have already confirmed. One declined, HealthBridge at the top said that they are discussing plans for a query model currently but they don't have one deployed yet, so it would be premature to be asking them to present material on that. Do we have the folks from MITRE on the phone, Linda or Omar? I don't know if they're – I know we have a couple of additional folks who have chimed in that they are able to come, they may – I'm not hearing them, so hang on.

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

Hey Deven, this is John Houston. ClinicalConnect, which is mine, is going to attend.

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

ClinicalConnect is one that is definitely coming. Hold on a second, I will give you other additional ones. Rhode Island is also confirmed, so there are two more confirmed, so we're doing pretty well so far.

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

Hey Deven –

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Deven, this is MacKenzie, I'm showing Linda is logged in on the phone, so maybe she's just on mute. Linda, are you there?

Linda Koontz – MITRE Corporation

Yes, I'm here, but I think Deven got the additional...

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

I just covered it MacKenzie.

Linda Koontz – MITRE Corporation

So, we're good.

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

Go ahead John.

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

Back it up to the one slide, the diagram you put up, if you could for just one second. Do we want – I think there are two different scenarios here that deal with non-targeted query. One is with, I think, within a HIE and then one is actually between HIEs and I don't know if you want to get into that complexity, but I think we're seeing very quickly that we're going to find that there's both inter-HIE and intra-HIE types of non-targeted queries. We know sort of where the patients at, but it might be in a different HIE, so I'm just wondering whether – does that make it too difficult or is that –

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

Well honestly I think that this particular diagram, and I don't think we should get too caught up in it, shows the concept of when you need to query an aggregator service –

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

Okay.

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

– which is going to be the case for querying whether it's within one HIE or whether you have to reach across whether to query another – if you're doing HIE to HIE, there nevertheless has to be a way for the query to hit the service that might have the index for the patient records. And whether that's a shared query or whether there is a way of organizing that, this is just trying to capture the simple concept of, some patient's information is sent to an aggregator service in order to try to locate the location of the patient's record. We do have HealthWay confirmed to testify and they have HIEs that are members of their network, so we'll have an opportunity to learn a little bit more about that model from them at a minimum, there may be others, too.

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

Deven, this is Judy. To me the edges are a little blurry so I'm going to ask you some questions to try to clear them up if you don't mind.

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

Okay.

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

One is, if the vendor itself is keeping track of that information, is that an aggregator service that you're querying or is that not because it is the EHR vendor itself?

Paul Egerman – Businessman/Software Entrepreneur

Judy, what do you mean where the vendor is keeping track?

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

Well perhaps the vendor is also the service, basically, but it could just be the service for its own products, so EPIC or Cerner or Allscripts or whatever is keeping track of all its aggregation of patient data, maybe not everybody else's, but maybe its own. It's not that it's querying someone else, it's querying itself, is that an aggregator service or is it not?

Paul Egerman – Businessman/Software Entrepreneur

No, I don't think so –

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

I was going to say the opposite Paul, this is Wes, I think it is an aggregator –

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

I do, too.

Paul Egerman – Businessman/Software Entrepreneur

I don't think so –

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

That's why it's a messy – that's why I said its fuzzy lines there.

Paul Egerman – Businessman/Software Entrepreneur

The issue is the concept of an aggregator service is that there is some intermediary between when you do the inquiry and when you get the actual result back that intermediary helps you find where the patient –

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

And that intermediary is the service provided by the vendor –

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Yeah.

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

– in this case and –

Paul Egerman – Businessman/Software Entrepreneur

I don't think so.

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

– in fact, they represent – I mean, the important thing is that it represents a query across multiple organizations.

Paul Egerman – Businessman/Software Entrepreneur

No, I don't think so, my understanding is that the environment that Judy's describing, the vendor's not involved with each individual inquiry.

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

The vendor provides an automated service –

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

It's – service –

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

I mean, that's true and for every single entity that we're asking to testify, they have a vendor who deploys this capability for them.

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

Right –

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

And so the question is, if the vendor isn't another party, but the vendor is the EHR vendor itself, and it's not everybody in the area, it's limited to its own –

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

You can make all kinds of fine distinctions, but I think the courts distinction that's most important to the patient is have they pre-identified the source or not and then there's these sort of degree – intermediary positions, well we've pre-identified the city or the market or something like that. But to me, I mean no – I seriously doubt that any aggregator service proposes to really have all the providers that the patient has ever seen. It's a case of whether, am I saying University of Pittsburgh Medical Center or am I saying Pittsburgh or am I saying anywhere in the country, I mean –

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

Well, and the reality here Wes is that because we're looking by patient and we don't know where that patient has been previously, it is a query looking for Deven McGraw.

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

I underst – it's always a query looking for Deven McGraw, assuming she's the patient –

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

Of course.

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

– but the distinction, from the point of view of the patient, is how wide is the net that's cast. Do I know in saying, yes you can get my data that I'm talking about the data that happened in my adult life at where I've lived in Pittsburgh. Or does it include the wild time I had in my 20s, do I know that when I went to Las Vegas for a procedure I didn't want people to know about that that will be – that that's potentially going to be included or not. Or, on the other hand, do I really not remember where I'd been seen and would I rather cast a wider net. I mean, from the patient's point of view, those are the issues.

Paul Egerman – Businessman/Software Entrepreneur

Those are good questions Wes. Again, we have to keep remembering we're talking about what it says on the bottom of your screen, non-targeted query.

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

So, I mean, he gets that Paul, I think he gets – I think Judy...I heard Judy's question to be, whether the sort of service that helps locate the patient's records, whether that could be provided by a single EHR vendor across sort of its multiple customers, and I don't see why it couldn't.

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

Well it's a little bit like –

Paul Egerman – Businessman/Software Entrepreneur

...it could be, but that's not really the way care everywhere works. This diagram is to show that there is some independent entity that has –

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

Why – then maybe the diagram's wrong. I mean, what – why –

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

There is a difference between an HIE, which is a repository and direct and to some extent Wes, we are –

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

– the direct is about –

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

– saying that –

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

– push, this is about query.

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

Yeah, I understand.

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

If I could make one simple suggestion for this diagram, it would be to draw a different colored arrow from the patient's current provider organization up to the very top of the patient's other provider organizations and that would be targeted and everything else would be non-targeted.

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

Except we're not trying to put targeted query in this diagram at all.

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

We're just trying to explain what a non-targeted query is, it's not a targeted query, okay. But I think that the distinction that Paul is raising, apparently, which is that there needs to be a third independent organization providing the aggregator service is not the most important distinction for the issue we're discussing.

Paul Egerman – Businessman/Software Entrepreneur

But in fact, it is the important –

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

It doesn't matter whether those are all provided by the same vendor or, I mean, is it all one product? Is it several products? Could it be RelayHealth connecting to multiple McKesson Hospitals? I mean, it's – sort of the independence of that central organization has not, in my mind, ever been part of the definition of targeted query and certainly not the value of the topic.

W

Can somebody put their phone on mute please?

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

Yeah, thank you.

Paul Egerman – Businessman/Software Entrepreneur

Very noisy.

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

This is David. I'm with Wes. I think that the fact that an aggregator service is taking in PHI and building some kind of an index, be it record locator or MPI or DEAS or whatever, is what's at stake here, not who happens to be running that service and whether it's the same vendor as the supplier of the EHR. I mean, those are important questions, but I think the focus here is on non-targeted query, which means you go through some kind of business associate that is performing an aggregation look-up match capability, and that's the only distinction that we've really focused on in the – either the patient knows exactly where the record is or they don't. And if they don't, it's an aggregator non-targeted query.

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

Right.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

I agree. This is Dixie, I totally agree.

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

Yeah, I think so too. So does the diagram just confuse people or does that help illustrate that concept?

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

I think that the diagram is helpful, but it's incomplete, so depending upon how much one reads into the diagram to be proscriptive, it could be harmful. I mean, in other words this kind of implies that the data goes out and then it comes back through the aggregator service, and that's not necessarily how it's done and – on the aggregator merely brokers a peer-to-peer conversation, that would be how many of the people who are going to testify do it. They don't go back through the central service. So, it could be taken – if it's taken to be too precise a diagram, it could be misleading. But all diagrams can always be that.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Yeah, I think it's simple to understand and I think we just described that they don't need to be in different physical locations. But I think the diagram, you don't want to make it too complex, and I think it's simple and depicts the right point.

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

Well and frankly, I'm personally – I don't want anything to confuse people. I mean, we need conceptually to convey what we need to convey in order to be clear about what we're seeking testimony on. If the diagram runs the risk of looking to proscriptive or being overly confusing, because in fact, we are not trying to create a schematic that covers every area, we were just trying to sort of hit the basics here.

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

This is David –

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

You could just eliminate the notion, from this diagram, of the aggregator service altogether and just –

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

Well take away the word service.

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

Oh, so just aggregator?

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

Either just aggregator or something else, because it was the word service that made me think of my question to begin with.

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

Okay.

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

Deven, I don't have any problem – this is David – I didn't mean to imply I don't like the diagram, I just pointed out that it can raise questions as well as answer them.

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

Yeah, I think that's a judgment you have to make whenever you try to introduce something simply, a hundred words is better than a thousand. I'm in favor of the diagram, I don't care if the diagram changes at all, and I think we need to be careful in listening to testimony that somebody didn't interpret it differently. And –

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

Well can I ask –

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

– I've got a question about the basic agenda though.

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

Okay.

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

We've got how many questions? How many testifiers? How much time?

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

Well, so let me go to the agenda, so you can see how we've sort of divided it up. So we're targeting eight, so that would be two panels of four apiece.

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

Okay.

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

And we are, at this point, giving them five minutes, but certainly, there's a little wiggle room to extend that time, but it's usually our tradition that we give them five minutes to present on key issues and then we try to solicit some of the other information by questions. So we have some opening framing, but we hope to get into the first panel by 1:10, starting the Q&A at 1:35 to the next panel begins at 2:15, so I guess it's not a huge amount of time for questions, but some. Then another Q&A and then we have – we have about 20 minutes at the end plus some – and it's 1 to 4, so there's actually plenty of sort of slack time at the back end with giving ourselves 20 minutes to wrap up and 20 minutes for public comment, when we don't usually get much of that. We might get more as part of a virtual hearing, but I don't know that we'd get 20 minutes worth. So we can build in more time on the panels, we can give everyone each another minute, we can try to make sure that we stick with no more than eight and if we have any additional folks who decline, we might even consider not going to some of our back up lists.

Leslie Francis, JD, PhD – University of Utah College of Law

Deven, this is Leslie from NCVHS. When we did our roundtable recently, we found that that format worked. The hardest thing was actually getting committee members to keep their questions short.

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

Well that's good to know Leslie.

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

We won't have that problem.

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

Deven, this is Judy.

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

Yeah.

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

And I would like to ask my second of the fuzzy lines question please. And that is, that the way it was described, it is that the patient has an index that points to where the patient has been, and that's what the service is, so you keep track of Deven McGraw has gone to these seven places, Wes Rishel has gone to these six places –

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

Not that I as the patient keep it Judy –

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

No, no, not you, but it's the index is per patient, so you have your name in there. And your name then points to the various places you've been. And you have my name and it says Judy Faulkner, the following 27 places or whatever. That's different than it says, these are the healthcare organizations within a certain region that is close to the patient's house or is near where the patient works, and we are going to do a direct query. So it's both direct and non-targeted and so –

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

We are not exploring targeted query here Judy.

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

Say that again.

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

So in other words, keep in mind the three models of query that ONC asked for us to look into, and they were a targeted query meaning you knew a provider that the patient had seen previously and you were targeting that provider, one or more providers that you knew the patient had seen previously, right. And so then we had two iterations of that, right, one query where HIPAA was controlled, no consent necessarily needed for that query and the other where there might be a sensitive data law that would be in play. And then the third model was this concept of non-targeted query, you don't know who the providers are and you're looking for that patient's record based on patient demographic information, using a service that will identify the location of those records.

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

Okay then –

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

To the extent you've got a patient list that's limited by geography or region or tries to guess the patient's providers based on an address. I frankly would consider that to be part of the policies that are adopted in order to assure an appropriate non-targeted query.

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

Okay, so that comes – well here's the problem then. That comes under – if that comes under non-targeted, in other words, I know that in this patient's area there are 12 different healthcare organizations, I will ask each of them –

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

Yeah, but you're still connecting it to a particular organization without the need to ask a service where the record is, and that's the –

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

– but the service is the EHR vendors own list.

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

Yeah, but that's not a query based on patient record, you're still targeting it to specific providers.

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

That's right we're targeting to specific not based on the patient's record –

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

Right, and that's what distinct between –

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

But here's –

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

– previous models and this model.

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

Here's the problem I have with what you just said though. You said you don't know where the patient has been, but in this particular case, the aggregator information does know where the patient has been, the patient has been seen –

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

Well they do, but that is information that's provided by the aggregator service –

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

Ah.

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

– after it's been queried based on the patient's demographic data.

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

So then what we have concluded is it could be the – it doesn't have to be a separate service, it could be the EHR itself, but if it is that you ask each one, rather than you know this is where the patient has been, that's the line that draws the difference.

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

Well –

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

This is David. To me – go ahead Deven.

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

No, I'm giving up, because I don't think I'm understanding Judy's question.

Paul Egerman – Businessman/Software Entrepreneur

Yeah and this is Paul. The issue is, even if you ask every individual physician one by one in the country that would still not count as non-targeted query. The non-targeted query is you ask something in the middle to guide you as to where to go and that something in the middle we've been given examples of an indexed approach where it has like a record locator. But there are also HIEs that actually centralize, actually contain the data, and there are various hybrids where they contain the data and they have pointers that contain some segments of the data and they have pointers. It's almost like thinking about like an Internet search, if you were to search on Deven McGraw, you could use like Google or Bing or something that would be like the aggregator that would find the data. Or if you happen to know the web address there, so the places where Deven McGraw works, you could just go directly to those web addresses.

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

But in that case, this is David, why are we focusing on limits to the query?

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

Because the Policy Committee asked us to David. We initially –

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

Okay – well, does that mean

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

– we came – and they were asking a lot of questions about well who can query and what do these models look like and what gets returned as part of the query and how does it work, and that's why we're doing this.

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

Okay so I would argue that a broadcast to every EHR in a country that returns is within scope of that question, and that it has nothing to do with the aggregator service, necessarily. I mean, of course nobody's going to do a broadcast, but just pushing –

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

Why are we speculating about this?

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

Because –

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

We're looking for real life examples to explore in order to be able to inform the Policy Committee. When we initially said we have, through existing law and what we have already said about targeted query, sufficient policy guardrails around query, we don't need any more. And they were not comfortable that we had done a sufficient amount of homework in exploring the models that existed out there and how they were operationalized, what they allowed and what they didn't allow in order to surface that question. And that's what we're doing, no more, no less. We are looking for operational models, no theoretical possibilities, in order to understand more about how this is deployed and then ask the next question about whether we need additional policies around this. Because we initially said, we don't and the Policy Committee was not convinced based on the work that had been done to date of exploring the actual models that exist out there.

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

So this is David again, so I agree, that's a helpful reminder, I appreciate that. I'm only suggesting that broadcasting out to a larger number of places in hopes that you might find part of that patient's record would fit their question, that that would be subject – that approach, it doesn't require an actual – well, it has to have some central service to know where to broadcast to. So maybe it's a moot point, maybe the central service in that case is just simply a registry of associated institutions that you're comfortable broadcasting to, in which case it is an aggregator and I withdraw my comment. I think that would keep it within fitting of your diagram.

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

Okay.

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

So then it's not hypothetical, if we have a list of the healthcare organizations around where a patient lives, and the patient may or may not say I went somewhere but I don't remember its name. And if we then go targeted to each of those in some geographic area around there, does that fall, given the discussion we had right now, that we are keeping this list of places and does that fall under targeted or not targeted, I really don't know the answer.

Paul Egerman – Businessman/Software Entrepreneur

That's targeted.

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

I would say that it's non-targeted.

Paul Egerman – Businessman/Software Entrepreneur

That's targeted.

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

It's targeted.

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

But how can be it be targeted?

Paul Egerman – Businessman/Software Entrepreneur

One phone call is targeted, you make ten phone calls it's targeted, make a hundred its targeted. Only non-targeted if I call somebody else who then tells me who else I should be calling.

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

I think that's too –

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

Again, I have to say that to me, I think Deven's argument that we only need to look at operational models makes this discussion moot –

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

Yeah.

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

– but if we're going to discuss it, then I think that the way to look at it is from the point of view of the patient. And either the patient knows where you're getting the data from or they don't.

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

That seems like a good metric.

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

So here's my suggestion. I mean, it's a good question. We are a week from the hearing, we have invites out to eight entities with a series of questions. Judy has – and Wes and others who have been active in this discussion have proposed a sort of another way of sort of looking at whether a query may not be something that the patient necessarily expects. Right, because the patient didn't say, well here's the provider I've been to in the past, they said nothing or they said, I've been somewhere but I don't remember who it was. And then there's a service like what's involved in EPIC that enables – has the capability to try and find that record, not necessarily through an aggregator service, but by querying likely providers – potential likely providers based on address.

I mean, I think we can think, as we are sort of getting the feedback from the entities that are deploying at least the initial models that we were targeting on some of these questions. I think that we've got some room to be thinking about sort of other models, given the sort of patient expectation framing in terms of our own consideration about what, if any, additional policy recommendations we would make on how to use a model where you're looking for a patient's record.

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

Deven, this is Leslie. It seems to me the really troublesome case is where the patient saw a provider and didn't want others to know that he or she saw that provider and a query turns it up.

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

Well, and that's one of the reasons why we have a lot of questions about sort of deploying meaningful choice and is there any sensitive data in those –

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

That could be an issue about sensitive data, it could also be an issue that you don't want your primary care doc to know that you might have been unhappy with care you were getting, so you went to see somebody else.

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

Oh, right, right, right. Umm –

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

– what if the patient tells you – what if you ask the patient can I look around for your records, and the patient says sure? Is that targeted or not targeted?

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

That's not targeted, I mean – that's

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

That's not targeted.

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

Yeah, it's – the patient –

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

You don't run into the surprise of the patient saying I didn't know you were going to do that, because –

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

Well yeah and I think the patient may have very good reasons for agreeing to a non-targeted inquiry.

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

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems
But once it's agreed to, it goes against what you were saying Wes is, patient –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated
No, I believe that the distinction is not – it certainly is helped –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology
Someone, mute your phone!

Paul Eggerman – Businessman/Software Entrepreneur

This is Paul. Here's what I suggest. We actually talked about this case already. We've talked about whether – what happens if you can make a large number of targeted queries, whether or not we should put any policy restrictions on that. And we talked about before, we came to a previous answer was no. But what we could do is we could revisit that discussion after we have this hearing.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated
Yeah, I don't think – yeah –

Paul Eggerman – Businessman/Software Entrepreneur

Because what it seems to me is people are uncomfortable with the way we resolved that issue and –

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

Paul, I don't think – I think it's that when we're – as is always the case, when we try to put particular boundaries around any set of policy questions that we ask that are based – there are always a lot of different models out there that become – that sort of blur the lines, I think, as Judy said, when we try to sort of cabin this. I think we are conceptually agreed on what we're trying to explore here. I think we have to be very careful to try not to have tunnel vision with respect to specific technical models of doing this and try to – and Judy, you're right, in some cases it's not going to be a surprise to the patient. That's not – that was not the right way to frame it, it's more about sort of looking for a patient record in a case where you don't know the patient's previous providers and there are likely lots of ways to do this.

We're going to ideally hear from eight different models, but we have some experience on our own Tiger Team that will help us as we explore the policy issues a little bit better. And I think we should just be careful not to get sort of caught – too caught up in the sort of specific lines that are drawn because frankly I think the questions are asked in a broad enough way that we can get at a range of policy issues that goes beyond – well beyond any particular model.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Deven, this is Dixie. I have a question.

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

Uh huh.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Wes and David and I have – through our work on the NwHIN Power Team, we've been recently looking at some standards for Blue Button Plus pull –

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

Okay.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

– that includes query, query for a record. And I'm wondering whether this hearing is confined to queries from other – from within the health system, other covered entities or whether it would also include instances where you might have a smartphone app that goes out and is querying for an individual's data.

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

Yeah, but those – that's per patient direction, under Blue Button Plus.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Yeah.

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

I think that raises a different set of issues than a provider looking to treat a patient, trying to find a record. That's a different set. I mean, it will be interesting for you to bring those experiences to bear in the policy conversations here, but there you're talking about not permissive disclosures of records, but records disclosed that the patient has an absolute right to and that's a different dynamic.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Yeah, yeah, it is. But the general question of whether we are assuming that the query is from another provider, let me make it –

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

We haven't, I mean we actually opened that question right up Dixie. We say, we – initially we approached this issue coming from sort of provider for direct treatment issue, but if you allow queries for other purposes, we want to hear it.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Okay. Okay.

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

Yeah, I have to say that's actually a pretty big issue. I mean as long as there are lifetime maxima on health plans, this is going to be a sensitive issue for some patients.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Yeah.

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

Okay, does anybody else have some suggestions on the actual agenda, whether other things need to be cleared up before you think we can move forward with this. I am now thinking, based on concerns expressed about whether we have sufficient time to really explore – to have good conversations with these folks that we're asking to be on the phone with us. But maybe we ought to take some of the time that we've reserved at the back end and build it into the actual body of the hearing. Because we will have subsequent Tiger Team call in July to go back through what we learned and talk about this. I mean it's always nice at the end of a hearing to have some time for people to share their thoughts after having heard all the conversations right in that moment, right. But I don't know that we necessarily need to reserve the amount of time we have reserved.

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

I think another strategy to consider is picking specific questions for each of the panels that are different.

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

Well, except then we'd have to know a bit more about their models so we could make good assignments –

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

Yeah.

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

– and unfortunately I don't think we have enough homework time for that.

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

Yeah, okay.

Gayle Harrell, MA – Florida State Representative – Florida State Legislator

This is Gayle. I think it's most important that we hear from the presenters in order to have our conversations later –

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

Okay.

Gayle Harrell, MA – Florida State Representative – Florida State Legislator

– we are there to listen to what they have to say, your questions are very, very carefully worded, we need to give them as much time as possible. We can talk until the cows come home later on.

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

You think?

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

Can I suggest though to Wes' point though, because I've already looked at the questions and I know our group is going to present is maybe ask them to focus on four or five that are most germane to them –

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

Okay.

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

– because this is a long list of questions and if you try to answer all of them, it might get –

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

Yeah, yeah, that's part of my concern is people –

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

Yeah, well we definitely were giving them the option to answer the ones that were most pertinent, I'm not sure we said specifically four or five, but we acknowledged right up front in the invites that it was more questions than they could cover.

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

Yeah, so, I just want – I think we should again make sure that's clear –

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

If there any final instructions going out, just re-emphasize that point, I think.

Leslie Francis, JD, PhD – University of Utah College of Law

It might also be useful to have a quick conversation with each to see which question their going to look at – this is Leslie, because what you don't want is everybody answering the same one.

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

Good point. It's – Linda, are you, can you come off mute for a minute? So this is Linda Koontz from MITRE.

Linda Koontz, CIPP/US, CIPP/G – Senior Advisor Privacy and Strategy, MITRE Corporation

Yes.

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

Yeah, is that something that you can – I mean you were already planning to have prep calls with each of the –

Linda Koontz, CIPP/US, CIPP/G – Senior Advisor Privacy and Strategy, MITRE Corporation

Yes, we've offered to each of the presenters that accept that we'll sit down with them and go over their testimony in advance. And we can make sure that we re-emphasize several points when we talk to the presenters, the time limit and also re-emphasizing that we want them to focus on the most important questions in their view and then we can make a point of having a little pre-meeting with each of them if you think that would be important.

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

Well right, and maybe even – it out, as per Leslie's suggestion and Wes' previous to that, that we try to sort of find out what they intend to focus on so that we're sort of getting all of the questions addressed in some way, shape or form and we don't have everybody addressing question 6.

Linda Koontz, CIPP/US, CIPP/G – Senior Advisor Privacy and Strategy, MITRE Corporation

Okay, we can do that. Thank you.

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

– randomly asked I can't even remember which one is number 6, but, by way of example.

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

You can certainly just use ditto.

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

Yeah, well exactly. Yeah another reason not to require a bunch of stuff in writing ahead of time is that they have the option of just reacting to what they heard previously and adding on to it, so, if they choose. Obviously whatever works best for them. Okay, other thoughts? I hope – I suspect there will be some of you who won't be able to make this, because it wasn't – hearing, because it wasn't part of sort of our pre-scheduled calendar, but there is always a transcript for this if you can't make it, Leslie, and I think you said that you could not. I suspect you won't be the only one.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Deven, this is MacKenzie, I was just reminded that the last time that we did a virtual hearing, we used the raise your hand function for the committee members to answer questions, do we want to go ahead and do that again for this virtual hearing?

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

It helps. It keeps us – because I can't see people with their tent cards, Paul and I won't be able to see those, that's like a virtual tent card.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Right. So I can send around the email again that describes the process to everyone, just so –

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

That would be great. Thank you.

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

– we don't have a lot of people talking over each other at once.

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

Okay. Yeah, that would – and it is – the benefit of this – benefit or downside depending, I guess, on how you look at it, it is just the Tiger Team this time, not Tiger Team plus another workgroup. Although I certainly made announcements at the Policy Committee meetings for anybody who wanted to participate in this who's not on the Tiger Team, they're welcome to listen in. But there may be fewer of us than has been the case for our other virtual hearings, the ones on identity, for example. Okay. All right, does anybody have something else they want to bring up at the hearing, otherwise I'd like to sort of move to begin the talking about the task that we assigned to a subgroup, and those of you who did volunteer for this are listed, but everyone is welcome to stay on.

And that is sort of thinking about Meaningful Use Stage 3 and whether there are methods beyond attestation to call greater attention to the HIPAA requirements that we have tried to spotlight in previous stages of Meaningful Use, and that's the security risk assessment and arguably also maybe addressing encryption of data at rest. But most of our conversation on this topic was about how important the security risk assessment was and how while it's required under – you have to attest to it in Meaningful Use, certainly the HIPAA audits are revealing that a lot of folks aren't necessarily doing this as completely as they should, or even potentially at all. So, is everyone okay with us moving into that now or does somebody else have something they want to mention on the hearing?

Okay, with that we will move into this quote/unquote, I'm making quotes with my fingers in the air here, "subgroup conversation," and everyone is welcome to stay. But for those of you who would prefer to allow this to be the subgroup that you didn't sign up for, you are free to go about your day. All right, so what we have here, and this is just a repeat of the question that was part of the Request for Comment that sort of initially teed this up for us. Just again to refresh everyone's memory, maybe a little bit more than I just have, the privacy and security is a category of Meaningful Use, and certainly has been for Stages 1 and 2. And that category has historically been used to sort of emphasize a couple of provisions of exist – that are already in the existing HIPAA Security Rule. The requirement to do or to refresh a HIPAA security risk assessment and address deficiencies that are revealed in the assessment, and then what was added in Stage 2, which hasn't begun yet, is addressing, not requiring but addressing the issue of encryption of data at rest. We had a presentation from David Holtzman about some high-level findings on the recent HIPAA audits about compliance with Security Rule generally and certainly was quite revealing to a number of us the – what they found with respect to Security Rule compliance.

So, we had a lot of discussion about, is there something beyond mere attestation that we can do in order to use Meaningful Use as a tool for assuring that this risk assessment gets done. We have, in conversations with ONC who are in regular contact with CMS, which is doing the audit for Meaningful Use purposes, this category is definitely part of what they are auditing. So to the extent that there is an entity who's sort of responses on Meaningful Use indicate that there might be something at issue, or whether they're part of a random audit, if they are being audited, this issue will be explored, whether they have actually done the security risk assessment. Including whether they have documentation showing that they've in fact done this risk assessment and what they looked at and what they found. So that's another piece of information relevant to this conversation.

The other interesting idea that was thrown my way at a conversation that – the eHealth Initiative hosted with a number of security officers from different healthcare systems across the country. It was a small gathering, it was probably about between 15 and 20 people, one of the security officials was really interesting. He said that there was a meeting about deployment of the view, download and transmit capability for Stage 2 in his facility, and he was not invited, as the security officer. And when he wondered why that was, given that they're deploying a brand new functionality, that does raise security issues, the response of the team that was gathering was, well, that's in a different category, the security risk assessment, that's category 5 and this is in category 2. So we don't really need to here, which I thought that was very interesting and I – who knows, maybe that's a one off from a particular facility, but it made me wonder whether the security risk assessment criteria could be made more effective if it wasn't off and on its own in a separate category. But wasn't tied more towards the other functionalities that are required for meaningful use. And maybe it's only the view, download and transmit capability that sort of raises a new set of issues, and it might not make sense for some of the other categories of meaningful use, but it did – I thought it was a very interesting comment and I wanted to share it with you all as we think through this issue.

The other suggestion put on the table for your consideration is for CMS to make it more clear, such as through frequently asked questions on what the expectations are with respect to the risk assessment and the importance of conducting and documenting that you've done the security risk assessment. And that certainly in the event of an audit, that documentation would be expected to be produced and certainly there could be links to some of the materials that both ONC and the Office for Civil Rights have put out on how to do an effective security risk assessment. Another potential idea, and again, these are all straw responses, is to instead of just to check the box attestation is to ask for meaningful users to identify the individual or individuals who are responsible for the security risk assessment. And then. I guess there could be another criteria that would sort of say, well you can't do attestation, you instead need to submit the documentation and it gets reviewed by someone, such as CMS or the Office for Civil Rights.

And I did not include that option on the straw responses because I do not see a requirement like that that requires an additional sort of review of Meaningful Use materials before people can be paid as something that's like to pass muster with CMS. But it certainly can be on the table for purposes of our discussion. I wanted to put up three that I thought had – were potentially improvements that might have the chance of sort of getting through the Policy Committee and then potentially being included. But again, I didn't intend that these straw responses to be limiting, I'll open up the door for other thoughts as well. Again, I think the central idea that we're trying to get at here is, how do we use Meaningful Use as a tool to not just shine a spotlight on the need to do this, but maybe make that spotlight a little more effective.

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

Deven –

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

Yeah.

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

This is John Houston.

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

Hi John.

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

I'm going to do a little verbal thinking here, but my organization, we've really looked at sort of two strategies in order to accomplish what you're talking about, and I'm just wondering whether some of this can be generalized. One is, we used HITRUST as a vehicle to ensure we had appropriate HIPAA compliance and I'm wondering whether some type of third party assessment that was along a certain – met certain criteria might be a good way to be able to demonstrate compliance for meaningful use purposes and would have some value from a certification perspective. And the second thing that we did as well is when the OCR came out with their audit plan for auditing covered entities for HIPAA compliance, we actually had our internal audit staff go through and literally run the audit plan and do a formal audit that was presented to the Board. So both of those, in my mind, are ways to have some level of independence that in fact you're going beyond simply checking the box that says you've done something for meaningful use certification. I'm wondering whether those are ways to maybe tackle this type of issue.

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

Would you require all meaningful users to be independently validated?

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

Well nothing would be required, but it might be one way that they could be validated such that if anybody ever came in to audit for certification, that this was sort of de facto evidence of your compliance with this.

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

Oh, interesting.

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

This is Leslie. There are also attestations and attestations. There are ones that simply check the box and then there are ones that kind of lead you through what you need to have done.

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

Well HITRUST will give you that and you can do a self-assessment with HITRUST or you can have somebody, a HITRUST certified auditor come in –

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

Right.

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

– and do it as well, which leads to Leslie's point which is, you can do this on the cheap by going the HITRUST process, and that gives some additional credibility. Again, it wouldn't be an absolute, but I think it would give a higher level of confidence.

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

This is Wes. I don't think that there's any possibility that CMS will ever publish a regulation requiring HITRUST.

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

I'm not asking for that, just not required.

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

Well, then I don't know what we could say in our expanding the floodlight or whatever we're doing here about HITRUST.

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

What I'm trying to do is propose that if you did this, let's just say an organization chose to go down the HITRUST route, that that would give some additional credibility in a certification environment, if somebody came in from a meaningful use pers – for meaningful use purposes came in to audit your certification.

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

I mean, I'm a big fan of HITRUST, but one of the credibility issues it has is it started out advertising itself as a safe harbor for HIPAA enforcement, and it's not a safe harbor. And given that it's not an SDO, there's very – there's just no possibility, I think, that CMS would ever imply anything about HITRUST, even if they believed, as I do, that it's a good framework. I think that we have to look at a) the framework for meaningful use – qualifying for meaningful use funds is attestation. As somebody pointed out, some attestation requires submitting supporting data, others requires checking the box under penalty of fraud. We could be – do something as simple as – and what has happened so far in Stage 1 and Stage 2 is just that essentially redundant, literally redundant features of HIPAA enforcement were called out and required for attestation –

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

Yup.

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

– as a focus. I think in Stage 3, we've probably got a couple of options, one would be to require submission of the risk assessment. A second would be to add some minimal amount of data that's required to be submitted, such as the identity of the person responsible, and presumably, a signature by that person.

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

Right.

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

And a third would be to find another area to floodlight. Myself, when I heard how good we were doing so far, I felt like well we needed to brighten the floodlight on what we had –

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

Yeah.

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

– not widen it and therefore dim it.

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

Yeah well, and honestly Wes, the conversation that we have had with the full Tiger Team on this issue was definitely heading in the direction of brightening the floodlight on what we had so far. Which notwithstanding that we repeated the question about whether we ought to add more to the list, we formed a subgroup to talk about whether there was a way to brighten the floodlight. It's just – it's not the most perfect metaphor, but it's the best one we have.

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

Yeah. Well another question, and Deven you are way more familiar than I am with the regulations, but, to what extent does a HIPAA security analysis cover – I'm sorry, HIPAA risk analysis cover conformance with the privacy regulation?

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

It doesn't.

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

Okay, so –

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

Not really, I mean, so David Holtzman, you hopefully are still on the phone, you can step in if I'm stepping in it here, but it's supposed to be a security risk analysis related to sort of the provisions of the – do you have technical, administrative and physical safeguards to meet the risks. Which sort of requires you to go through – I mean, you might use the Privacy Rule to consider what you can and you can't do with data, but at the end of the day, what you're assessing is sort of the threat to accessing – inappropriate access to data, and I guess the Privacy Rule provides some parameters. But it is not – you're not supposed to do an assessment of your compliance for the Privacy Rule, you're doing an assessment of security risk and how you're – and what functionalities and activities and policies are you going to put into place in order to address your risks.

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

So it's not clear to me whether employee education about privacy falls under the Security Rule or the Privacy Rule, but there are probably – but if not, there are probably one or two things like that from the Privacy Rule that we can relate directly to specific requirements in the – within meaningful use, that might be worth casting a floodlight on. I think small practices employee education is an ongoing issue.

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

Yeah, and we – my recollection from our – is when we had the presentation from David Holtzman of OCR, it was on two issues, right. One was sort of on what are the education and training of sort of staff requirements in both the Privacy and Security Rule, because there are components of both. And then, what happened with the audits, high-level? But –

David Holtzman, JD, CIPP/G – US Department of Health & Human Services, Office of Civil Rights

So Deven –

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

– my other recollection was that we sort of thought that the requirements for training existed but would sort of be hard to shine a spotlight on using meaningful use. But we can also resurface those discussions in another subgroup call, as we consider this. I'm amenable to that. David, I interrupted you, go ahead.

David Holtzman, JD, CIPP/G – US Department of Health & Human Services, Office of Civil Rights

No, that's okay, I just wanted to let you know that I am here and that I agree with everything you've said. But I do want to emphasize that even in the audit protocols that you all have mentioned, we looked at the requirements of the Privacy Rule and the requirements of the Security Rule as two different categorical areas and in our experience, organizations do not integrate the policies to comply with the Privacy Rule to those of the Security Rule. In fact, we've impliedly encouraged organizations to keep two separate sets of policies, although we typically understand that the Security Rule supports the Privacy Rule, and to some extent there is some bleed-over, but they're two distinct and separate programmatic approaches.

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

So it sounds to me like if we were going to add anything to Meaningful Use Stage 3, it might be to, pardon the expression, shine a spotlight on privacy as oxymoronic as that sounds.

David Holtzman, JD, CIPP/G – US Department of Health & Human Services, Office of Civil Rights

Well, you run into perhaps a regulatory complication, but I'm not sure that that's a topic that we want to go into today.

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

Well I would say if we were going to run down – spend time running down an alley and discover it's blind, it wouldn't be the best use of our time. Maybe – is the regulatory complication something that is just you have to be deft in how you do it or is it just a blind alley – is this whole idea a blind alley?

David Holtzman, JD, CIPP/G – US Department of Health & Human Services, Office of Civil Rights

Um, you know what, I'd prefer to think this through, but I think as a policy matter, the folks in CMS had not thought – had not considered the HIPAA Privacy Rule to be a topic to be included in the Meaningful Use because it focuses specifically on health information technology and the Privacy Rule requirements would not extend to the vendors and developers. So, it's – it only applies to those organizations which are attest – that are receiving the incentive payments for Meaningful Use, but not apply to those organizations that are partners with them in the provision or development of the technology itself. Does that make sense?

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

In some ways it does David, I certainly can recall in very early stages of the HITECH Program, when we initially put forward some criteria for the privacy and security area for Meaningful Use Stage 1. In the proposed form, we as the Policy Committee had actually, after some pretty robust discussion, had suggested to CMS that anybody with a significant HIPAA violation, that they have been found to have committed, so not just an accusation, but a finding from the regulator, that they were willfully neglectful of the rules, or criminal – or there was a criminal violation that had taken place. So, only the sort of upper categories of violation, if this had happened to a covered entity, that they could not be eligible for a payment under Meaningful Use. And we recommended this as a criterion, and essentially what we got back from CMS was, we don't want to blur the lines between compliance with the privacy rule and compliance with meaningful use. There's already an accountability infrastructure in place for Privacy Rule compliance. But they were amenable to the security risk assessment being performed and to attesting it and probably because of its link to the use of the technology.

And not only that, but they were amenable – we were careful in what we recommended for Stage 2. And we stuck to the Security Rule and once again said, well, let's see if we can get another one through, and we said, how about attesting to addressing encryption of data at rest, given all of – given what we know now after implementation of the breach notification requirement about lack of encryption being deployed on portable media. And we got that one too. So, I think that's – if we're – we might be over-interpreting history here, or our recent experience, but certainly we have had better luck in getting CMS to include criteria in Meaningful Use that have to do with secure use of technology than we have at sort of considering the privacy – provisions of the Privacy Rule. So, for what it's worth.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Well this is Dixie, I have one thought.

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

Okay.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Your number three Deven –

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

Yes.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

– is – since our 2014 edition is really focused on exchange between and interoperability between organizations, and consumer engagement, we could maybe – those – if I were to argue for targeting the risk assessment for anything, those would be the areas I would target it toward.

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

Okay. So in other words, making it clear in those categories that the security risk assessment has to address any new functionalities provided as a result of deploying 2014 criteria in those areas.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

Yes. And the reason why it would make sense, well, a couple of reasons. Number one is really focusing it on something specific like that would maybe increase the likelihood they'd really pay attention to it, but number two is the HIPAA risk assessment, HIPAA is pretty internal focused, it has hardly anything outside. So it would strengthen their focus on those exchanges.

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

So what I'm going to – that's a really interesting idea Dixie. So, I think we've just begun this conversation within the subgroup, but we've got some interesting ideas that I'd like to sort of massage a little bit further into some more meaty straw responses, because I think there's more that can be built into even all three of these, and that they're not mutually exclusive, necessarily. And we'll also resurface all of the slides from David Holtzman about – that we were – that were part of his presentation on not just the audit results – high-level results, but also the training provisions of the Privacy and the Security Rule, so that we – so that in case we want to revisit those, we will have that material with us and we'll schedule another time to talk about this. Does that sound like a way to move forward? And John, your suggestions I think I can – I actually – without necessarily requiring something to be submitted to CMS or giving someone a specific safe harbor for utilizing a third-party assessment, I think there might be ways to think about how to expand some of the FAQs that CMS provides to certainly incorporate the ability to use a third party service or to use checklists or to recommend the use of checklists, particularly any checklist that have actually been developed by the regulators.

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

Right. I'm just thinking for a way for organizations that have a desire to ensure that they're compliant and there are no issues, if they have somebody, something to go by, which I understand it won't be a safe harbor, but has credibility that – there's credibility to a process that would be proposed to give people a higher level of assurance that there aren't going to be issues with certification.

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

Well, I mean it certainly is a way to document that you've done something above and beyond what you could possibly do internally, but without suggesting that people would have to go in that direction.

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

I don't want to make it mandatory, but I think the voluntary aspect of it to me is very attractive.

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

All right, any other thoughts before we move to some public comment? Thank you everyone, really helpful thoughts here. Okay, MacKenzie, can you open up for public comment please?

Public Comment

MacKenzie Robertson – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

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

Caitlin Collins – Altarum Institute

If you are on the phone and would like to make a public comment please press *1 at this time. If you are listening via your computer speakers you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. We do not have any comment at this time.

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

All right, terrific. Thanks everyone and we'll talk to you next Monday, if not sooner.

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

Thanks Deven.

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

Okay. Bye.