

**HIT Policy Committee
Privacy & Security Tiger Team
Transcript
April 30, 2013**

Presentation

Operator

All lines are now bridged.

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

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 at the end of 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 – Center for Democracy & Technology – Director

Here.

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

Thanks Deven. Paul Egerman?

Paul Egerman – Businessman/Software Entrepreneur

Here.

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

Thanks Paul. Dixie Baker?

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

I'm here.

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

Ah great, thanks Dixie. Neil Calman? Judy Faulkner? Leslie Francis? 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 – Federal Advisory Committee Act
Program Lead**

Thanks John. David McCallie?

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

Here.

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

Thanks David. Wes Rishel? Micky Tripathi? Kitt Winter?

Kitt Winter – Social Security Administration – eHealth Exchange Coordinating Committee Chair

Here.

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

Thanks Kitt. And any ONC staff members who are on the line, if you could please identify yourself.

Kathryn Marchesini, JD – Office of the National Coordinator

Kathryn Marchesini, ONC.

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

Thanks Kathryn. And I believe we have David Holtzman on the line as well. Okay. So 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 MacKenzie. Welcome everyone to the millionth call of the Tiger Team, I think that's probably not quite right, but ...

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

We can start keeping track if you want Deven.

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

I want to thank everyone, all of our Tiger Team members for being on the call today and also thanks to members of the public who are joining us. We are going to try to do two things today. One of them is to wrap up our discussions on query response scenario 3, which really just involves making sure that we generally captured, with our language, the conclusions that we reached at our last meeting on the issue of whether there should be any other additional limits on non-targeted queries, which is scenario 3. We don't want to wordsmith on the call today, we can do wordsmithing offline if folks want to suggest some better language, but I want to make sure that we've at least captured the essence of where we landed on our last call.

And then, we have strong responses, then we're going to move into the discussion of the meaningful use request for comments on privacy and security issues. The particular pieces of that RFC that were delegated to us to review the comments on and to provide specific feedback on what should or should not necessarily be in Meaningful Use Stage 3, to the Policy Committee. We began this discussion on our last call, we hope to advance it today and we've created some straw responses to facilitate getting through those. If we're able to actually get through all of them today, we can report on them in the May Policy Committee meeting, which is next Tuesday. But we do have time, there isn't time pressure to complete this by the May meeting, and we actually have a call the day after the Policy Committee next Wednesday, if we need some additional time to wrap this up.

And then there's also a slide towards the end of the deck, if in fact we do finish talking about the RFC comments, to get your feedback on what our next topics will be, as a Tiger Team. And they come from the agenda setting exercise that we did earlier in the year, but it's just getting some feedback on sort of priorities for where we will head next. Paul, do you want to add anything to that?

Paul Egerman – Businessman/Software Entrepreneur

No, I think that's a great summary Deven, except to say, it does not feel like our millionth call, seems like we just started yesterday.

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

Oh, that's very nice Paul. Well said. Does anybody else have any questions about the agenda before we dive in? All right, here we go. So just to remind folks about what scenario 3 is on query and some of our prior recommendations on this topic, this is non-targeted query for direct treatment purposes, the circumstance where you don't know the patient's previous provider, so it's really you need to make an initial query to find where the patient's records might be. It may require the use of an aggregator service. And the first question that we addresses was whether patients should have meaningful choice about whether or not their included in an aggregator service that permits queries from external providers. We said yes, and the Policy Committee agreed with this.

What we left for ourselves to consider, because we didn't have sufficient time before the April Policy Committee meeting, was whether there should be any other limits on queries, such as by geography or by list of providers. And essentially what we had recommended was that we had already put forth a number of recommendations on queries that included providing individuals with meaningful choice, in the case of a non-targeted query and the use of an aggregator service. Requiring the use of audit logs for queries, which must be provided to patients on request, and all of the recommendations we made on scenarios 1 and 2, that were intended to create an environment to give providers some reasonable assurance in how they respond to external queries, consistent with their professional, ethical and legal obligations. So, assuming these get adopted, we didn't see any need at this time to establish additional policy to place limits on queries, but we might decide to revisit this if the recommendations that we meant, and I think arguably intended to appear as a package, would not be adopted or there are more nationwide query models in existence. We noted, on our last call, that many of the query models and use of aggregator services that exist today end up being naturally limited by geography because they're established by an HIE, an HIO in a state, for example.

So this was our capturing of sort of where we thought we landed. Again, because we had done so many other recommendations on query, we didn't see a need to create any other limits on non-targeted queries, because we thought we laid a sufficient foundation based on the circumstances that exist today and probably in the near future, although maybe not in the foreseeable future. So, absent tiny wordsmithing, which we'll take from anybody offline, but I'd prefer not to micromanage the wording, did we capture the essence of what we had agreed upon in this language or is something not right?

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

This is David. I'll start. I think this looks pretty good.

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

I agree, Dixie. Yeah.

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

All right. Terrific. Well again, we'll take – we have some really good editors on this Tiger Team, so if anybody wants to suggest any tweaks to the language, that don't disturb the substantive meaning, we'll definitely take them. But in the meantime, what we will then do is proceed to present this to the Policy Committee next Tuesday, at the meeting. Hopefully they will endorse it and then all of our recommendations on query will be part of a single transmittal letter that will then go officially to Dr. Mostashari, as head of ONC, and be posted on the website. Okay. Thank you all very much, we'll move into our discussion on the meaningful use request for comment comments, in the area of privacy and security.

So, our – just to remind everybody about what our goals are, our goal is to determine if there are any relevant policy considerations to discussion based on the feedback to the meaningful use request for comments. And that includes both on some issues that we deliberately teed up as a Tiger Team, as well as issues that were raised by others that included in the RFC. As we go through these issues, one of the things that we know is a possibility for us, and we want to consider, is whether the issues raised are not policy, but more ones of technology that should be sent to the Standards Committee, more than likely the Privacy and Security Workgroup, to consider. And we have the advantage of having Dixie and David and others involved in our Tiger Team, who would have to be involved in the discussions, whether they were taking place here or there.

So I think we'll be able to better – I think maybe even better come to conclusions about who's the best body to be considering this. Based on the circumstance of the question and/or maybe sort of divide and conquer, like maybe there are pieces of a question that belong to us, but others that need to be addressed by standards. And our goal really is again to finalize what the, what our recommendations would be from a policy standpoint for Meaningful Use Stage 3, in light of really, I think, all of the discussions that are going on within the Policy Committee on Stage 3. And frankly, including the desire to create a more streamlined approach to Meaningful Use in the third stage and also to be sort of trying to up that meaningful use escalator and be a bit more focused on outcome. So, I think we should have all of that in our mind as we're going through this.

And so what we're going to do, the way we're going to proceed in this discussion is to take each of the questions that was asked in the RFC, and talk about – we've prepared a straw response just to begin the conversation, but you're not bound by it at all. We're free to, as always, fully discuss this and come up with a response that we think makes sense. We built many of these straw responses around our initial set of discussions last week, but there wasn't a whole lot of time to go into detail on some of these, and so, some of them are frankly just our ideas about a way to kick-start the conversation. What you have in the background slides, the slides at the end, are the summary slides that were part of Kathryn Marchesini's presentation to you last week, where you can see the summary of the comments that were received. And then in an email several weeks ago, you actually received the whole files with all of the comments that were received in these areas. So, if you really wanted to dig into this in detail, you have all of the materials that enable you to do that. But we at least have on these background slides, the summary comments, in case we need to go and refer to them.

So this first question, actually the first couple of questions, involves the work that we had done on identity management, potentially both for providers and patients, but I think this first question may arguably be one, I guess it could go really for providers or patients, but we should talk about that. So the question itself was, "How can the Health IT Policy Committee's recommendation on reuse of – on identity management be reconciled with the National Strategy for Trusted Identities in Cyberspace and that approach to identification which strongly encourages the reuse of third party credentials?" And the straw response that we've provided here is essentially reminding people that in fact we deliberately incorporated NSTIC into our recommendations on identity management. And the straw response actually talks about this in the context of provider users, but we also did talk about the reuse of third party credentials for patients as well, and so we could augment this response to be complete.

I mean essentially what the straw response says is that we're reiterating our recommendations on identity proofing and authentication. Where we recommended, at least on the provider side, multifactor authentication for remote access, and other in access environments identified by the covered entity that might require multifactor identity authentication in accordance with their risk assessment. ONC should update its policies based on technological improvements and its work should continue to be informed by NSTIC, taking into account provider workflow needs and impacts on healthcare quality and safety. So this is literally lifted, almost literally lifted, from the recommendations that we did on identity management, that actually talk about how NSTIC is out there, working on reuse of third party credentials. But the – at the time when we were deliberating these issues, both for providers and patients, there really wasn't anything that we could point to as a solution that people could deploy and rely on at that particular time. So how do people feel, I mean, about just sort of reminding people that we didn't forget NSTIC, we just didn't think it was ready to be utilized for Stage 2.

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

This is Wes. I'm strongly with that position.

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

Okay. And maybe I can word it just that simply. We incorporated it; it wasn't ready for, at least at this stage, to be used.

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

Well I think that's a, this is John Houston. I think that's a valid comment to make that as NSTIC matures, we believe that it will provide a path forward on addressing identity management and third party credentialing and things like that. But I'd also, I'm reacting to the work multifactor in the straw man, given that we've talked a lot about multifactor, but I'm thinking that there's a better – going forward basis, especially with NSTIC, that there may be a better way to say that. Because I think we're really talking about advanced authentication that, and I hate to say, sometimes people get caught up in what multifactor is and they sort of have their vision of what it is and I'm a little afraid that that might be self-limiting.

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

This is Dixie. My one com – I had two comments but one of them directly relates to what John just said.

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

Okay.

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

When you actually read this Deven, you – I like the words that you used at the end of that sentence that said something like stronger authentication based commensurate with the risk assessment. I think those words would be better than what you have here.

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

Okay.

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

And the second is a minor thing you have identify proofing.

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

Oops. Thank you.

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

That's a new technology, you just don't know about it yet.

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

This is David. I'm wondering John, were you looking for a phrase like more than single factor as opposed to multifactor.

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

Yes.

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

Or were you ...

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

Because I think NSTIC may come up with some other things that, I'm not sure but that may not be what people's vision of multifactor is.

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

Right.

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

It's stronger – to me, I think stronger is better than multifactor.

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

Okay.

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

Yeah, or stronger than single factor or ...

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

Just stronger authentication, because there are multiple ways to authenticate identity and I just think stronger authentication message commensurate with the risk is exactly the right way to go, which is what she really read.

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

Yeah. Well, and we're really trying to reiterate what our recommendations were previously, not trying to change them in any way. Having said that, we're not trying to – we don't intend to just sort of stick them in whole cloth here, so we do have to find an effective way to summarize them. And all this language is helpful, that you guys are suggesting, to make it more clear and not be misleading to people.

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

And it's always good to remind them that all of this should be risk-based.

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

Right.

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

It's ...

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

Yes. Did I hear someone else trying to break in or that might have been my echo again. Okay...

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

This is Wes. I just, I'm – I had stopped because you were sensitive to making changes, but the most important thing I think to say, rather than single factor is passwords are ineffective, so I wonder if stronger than passwords would be better terminology, but I'm willing to say that's too much like wordsmithing and let you move forward.

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

Let's – we'll try to again, I want to – I don't want to make new recommendations on this, but I do want to articulate the summary in a way that captures what we said before. And as always the case, what's in this letter that's linked on the bottom of the slide here, discusses all of the things that you guys have raised. And inevitably, when you try to shorten it into something shorter, you leave some concepts out. So, I think we can do better in trying to sort of capture what we had said previously. And yet still making the point that we deliberately incorporated NSTIC into those recommendations and asked ONC to continue to follow it and look, when, for whether and when there are solutions that are ready to be deployed. That's when they could move forward on this. So ...

Joy Pritts, JD – Office of the National Coordinator

Deven, this is Joy. I don't know if this is helpful, but there are pilots under way in the healthcare sector at this moment. So, it may be a good point of reference to re-examine how things are going when the pilots are completed.

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

Are there NSTIC pilots, Joy?

Joy Pritts, JD – Office of the National Coordinator

Yes.

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

Oh, huh.

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

And how many of them are health-related again?

Joy Pritts, JD – Office of the National Coordinator

I think two or, one or two, there's one I'm sure of that I'm pretty familiar with, but I think you may be right, there might be a second one that has a healthcare component, but is not solely health.

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

Joy, this is Wes. I think Dixie and I, probably everybody would like to see you have any URLs or references to those, we'd like to hear about them.

Joy Pritts, JD – Office of the National Coordinator

I will see what I can find out for you, that project is being run out of NIST, and we have a member of my team who is very active in monitoring them. So, I will see what, when we will be doing an update for the Policy Committee in the next few weeks, and I'll see what we can do about including a slide or two on NSTIC.

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

Thank you.

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

That's great Joy.

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

Joy, this is ...

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

Does anyone object to having language in here about, that expressly references the pilots and that we could sort of reassess – we should monitor their progress and potentially reassess whether for Stage 3 that there might be something ready. Or is that too much ...?

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

This is Dixie. How about in that last phrase you incorporate as it matures, which would sort of get the flavor of pilot without limiting it to pilot?

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

Okay.

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

This is David. Is there a covert pressure to use meaningful use as a way to push NSTIC forward or is that just an aggressive interpretation of why the question keeps coming up?

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

David, I actually don't recall how this question landed in the RFC.

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

I mean it seems to me to be one of those things that when it works well, we're going to all jump on it, but the question is, are we trying to use meaningful use as a lever to push it forward faster than might otherwise occur. Which might not be a bad think in the long run, but I'm not sure it's really what we want meaningful use to be saddled with above and beyond all the other stuff.

Joy Pritts, JD – Office of the National Coordinator

David, this is Joy and I think that our office is instrumental in including this in the language in the RFI. And our concern has been that we make sure that the administration's efforts are aligned, so, we don't want to go off, headed off in a direction in NSTIC or in meaningful use, if the other program is headed in an opposite direction.

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

Got it. That makes sense.

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

Can I ask a more pointed question? This is John Houston again.

Joy Pritts, JD – Office of the National Coordinator

John, no, you can't, no ...

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

Aw, man. Let me rephrase my question as a comment, I'm going to ask a more pointed question. Is a part of this in order to ensure that NSTIC remains funded and/or a priority, because I've heard the mention of the fact that some people at least seem to be interested in deprioritizing it or at least that's the implication that I've heard.

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

I think we can deal with this question without necessarily opining on all of that.

Joy Pritts, JD – Office of the National Coordinator

Thank you, Deven.

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

I think it's, the question was there, comments were received in response to it. What we're doing, in our response, is reminding people that we have always appreciated the potential of NSTIC to provide us a solution here. And that we urged ONC to keep an eye on it.

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

And I agree – I agree with that statement, I think NSTIC is a very interesting way to – opportunity, and I wouldn't want to see it go by the wayside, and I fully endorse continuing to monitor it.

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

Yeah. Yeah, I mean, we're, in many respects, we're just reminding people of the position that we took and that the Policy Committee adopted on this issue. And it's an opportunity to reiterate it, but we don't need to say any more or any less.

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

I didn't argue that we should say more, I was just wondering whether ...

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

Okay. Yeah, frankly I've lost track of the Initiative. Because it's – at one point it was moving at a, I don't know, fast pace might not be the word, but being able to go to sort of 2 days meeting in Chicago or be on the phone for that period of time and, it was just a big effort, from what I understand. But it would be very interesting to hear about how it's progressing, in the coming months. All right. On that note, still on the question of authentication, the second question that was asked is, "How would ONC test our recommendation for two-factor authentication, this is exactly how it was worded in the question, in certification criteria?" And our straw response here is that questions around certification criteria and testing are not really about – are not about policy, but instead, are best answered by the Health IT Standards Committee Privacy and Security Workgroup, or at least the Health IT Standards Committee. Is th ...?

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

This is Dixie. We did answer this question, I remember, in the review. I think it's pretty straightforward, but I agree. I think it – the testing of technology better belongs in the workgroup, yeah.

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

Okay. All right, good. I like it when we can get something off our plate. We can put more on. This is another question similarly around certification, and whether authentication should be allowed as a stand-alone or an EHR along with an authentication service provider. This one was another one that seemed to us to be one that isn't in our bucket, but is instead in the standards bucket.

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

This is Dixie. I would agree, especially since this question is very tightly related to the issue that the Privacy and Security Workgroup brought up about modular certifications. So, I think that we did answer this one as well.

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

Okay.

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

I think the NWHIN Power Team may have answered this one, too. So, we've already, just as a matter of logistics, we've submitted comments on this RFC up to – and that was like months ago. So why, from the Standards Committee side of things, has submitted their comments.

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

Well so Dixie, this is a little bit different. This is not just your comments to the questions, but your review of all of the other comments that came in and whether that would change the comments that you made or have you modify them. Or, in other words, we're – the Policy Committee and the Standards Committee are working together to consider the public comments on the RFC, not just our own views.

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

Okay.

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

But what other folks have said, and then to do a second set of responses

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

Okay. Okay, thank you, I'm glad I asked the question. I didn't get that context, so thank you. So the Privacy and Security Workgroup should do the same sort of thing, is to look at those comments.

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

Yeah. And I think that's what's planned, although the staff on the phone can let me know if I'm off my rocker about that.

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

This is John Houston regarding this comment. Why can't we simply say that we believe that whatever provides for the best security and confidentiality is what we should be striving for, and if it – if having a third party authentication be certified separately improves that, then we're open to that paradigm.

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

Well that's a good question John. I think, customarily issues of sort of certification and I'm trying to think of sort of where the original notion of being able to certify modular, components of a certified EHR technology, whether that initiated to Policy Committee, the Standards Committee or both. I do know that the more difficult questions around the privacy and the security related functionalities of certified technology and whether those needed to be part of the sort of base EHR or could be done in a modular way was definitely one that was handled by the, largely by the Standards Committee, is my recollection. But ...

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

That is the right place to do it, I'm just saying, if we support the notion that if it passed privacy and security, we're at least in support of this being considered.

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

This is Dixie again. The – I think the whole idea of modular certifications came out of ONC, it didn't come from either of the Committees.

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

Oh.

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

But I would say that one of the biggest problems that the Privacy and Security Workgroup had with the initial approach of Stage 1 was separately certify each module. So every module would have its own security, which does not lend itself to strong security. The second, Stage 2, eliminated the security certification of modules entirely, and so our workgroup argued hard for bringing some level of certification of security to modules back in Stage 3. So, John's comment from the Policy Committee that whatever approach they take to certifying multiple modules together, however you want to phrase that, should strive for the strongest security, I think is a policy statement that would be well worth making.

Paul Egerman – Businessman/Software Entrepreneur

And – this is Paul – I think we're starting to get a lot of different things confused here. I mean the concept of modular certification actually was approved by the Policy Committee in the initial work with.

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

Your workgroup.

Paul Egerman – Businessman/Software Entrepreneur

What the certification, yeah, the Certification Workgroup came up with.

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

Okay.

Paul Eggerman – Businessman/Software Entrepreneur

Then we ran into some problems with actually implementing it, which is, how does certification of modules relate to security issues. And so there was a little bit of a challenge to figure that out, and as Dixie pointed out, we sort of went to two different, took two different approaches in Stage 1 and Stage 2. This question is a very limited question, which is, should ONC permit certification of an EHR if it's standalone or is it possible to include some third party service provider. And so, to me the answer to this is – in the straw response is reasonable, that the technicality to that are best addressed by the Standards Committee. And, you could say something more if you wanted to, as long as security is not diminished or is improved by that process or whatever. But to me, that should go without saying, I mean we've established some policy guidelines for authentication and so hopefully whatever approach is taken is consistent with those policy guidelines.

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

Yeah. This is Wes. We just have to keep in mind that the best security is not letting anybody into the system. We always have to – it's risk-based analysis. I don't know that any admonishment from the Policy Committee to up the security would be better than just recognizing it's a risk trade-off.

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

Yeah.

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

Yes, and the ...

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

This is David. I think you could interpret the question as a policy statement or policy question, is the use of third party authentication services okay from a policy point of view. And I think we all agree that it is, so maybe it's just endorse that there's nothing wrong with using a third party, as long as it implements the right security and meets the risks and all that.

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

Yeah, I agree with David. Why don't we just say yes, permit, I mean the way it's phrased is, should it permit, so, yeah.

Paul Eggerman – Businessman/Software Entrepreneur

Yeah, I agree, let's say yes and let the Standards Committee worry about it.

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

Okay. So, yes. That's short and to the point. Okay, moving to the next question. This one asks, "What, if any security risk issues or HIPAA Security Rule provisions should be subject to Meaningful Use attestation in Stage 3?" And just to remind folks the privacy and security Meaningful Use criteria that have been included in Stages 1 and will be part of Stage 2 for Meaningful Use, essentially are shining a spotlight on particular provisions that exist already in the HIPAA Security Rule. The requirement to do the risk assessment, which was the Meaningful Use attestation requirement for privacy and security in Stage 1 and that requirement again in Stage 2. As well as attesting to addressing the implementation specification of encryption of data at rest, so not requiring implementation of encryption of data at rest, but attesting that you have addressed it, consistent with the HIPAA Security Rule.

So those are the two provisions and what this question asks, and this is one that we actually did include, we as the Tiger Team included in the RFC, is whether in Stage 3 we should put this attestation spotlight on yet another Security Rule provision. And so one of the ones that we had specifically teed up for public comment was attesting to having complied with the requirements to train individuals that are part of the HIPAA Rules. I have them labeled here as part of the HIPAA Security Rule, but it actually occurs to me that requirements to train may actually be part of either both the Privacy and Security Rule and not just the Security Rule, and thank goodness we have David Hoffman and other staff on the phone who can help us work through this. But the idea was to shine a spotlight on an existing HIPAA requirement, noting that many of the enforcement actions that have taken place in the last couple of years have spotlighted a lack of training on the part of the entities subject to enforcement actions. We deliberately teed up as an RFC response putting the spotlight on the training requirements, and so we have included that in our straw response for your discussion today. And then I think there's a corollary question to that which is, is this the only attestation requirement or would we add this to stage – Meaningful Use Stage 3, so that then there would be three, risk assessment, encryption of data at rest and training. So, this one is all policy for us to discuss. Any thoughts?

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

This is Wes. I'm preparing to give a presentation on this right now, so, or get current on it. I think that the primary impact of meaningful use attestation is somewhat shifting away from the large organizations, which are experiencing enough other pressure on HIPAA and privacy and security, that attestation is more likely to be redundant. But very strong on practices, particularly smaller practices and...because they kind of fly under the radar a lot of the times, and I would agree that we should include training. And I would further assert, we should include all three rather than dropping the other two, because this may be the primary vehicle to raise the awareness in smaller practices.

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

I agree with\ – this is Dixie – I agree with him. In particular, I definitely would be opposed to dropping the risk assessment.

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

Right.

Paul Egerman – Businessman/Software Entrepreneur

And Deven, could you just sort of quickly explain training, who gets trained? What do they get trained on?

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

So, David Hoffman, are you on, able to help us out? What's already in the regulations on, what the requirements are on covered entities to train their staff? Maybe he's not there. Joy do you ...?

Paul Egerman – Businessman/Software Entrepreneur

I'm just trying to understand about this comment, if you're a solo practitioner, and you have 3 or 4 staff.

M

You have to train your staff.

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

Solo practitioner has to go to somewhere, maybe his professional association or her professional association and then buy a training course that he gives to, that his assistants have to take, would be my guess.

Joy Pritts, JD – Office of the National Coordinator

So, this is Joy. And there is a training requirement under the Privacy Rule, I'm trying to see right now if there is one under the Security Rule, I'm sure it is, because everything ...

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

Yeah.

Joy Pritts, JD – Office of the National Coordinator

... everything requires training. And the important thing to remember with this is that it's meant to be scalable and flexible. So what a small healthcare provider has to do to train their force is much different than what a large hospital organization would be expected to do. As a matter of fact, we have produced a number of materials, not to give a public service announcement, but that's what I'm going to do, on our website, in collaboration with OCR, that providers can use to help train their staff, small providers. Like how you secure mobile devices and things like that. So that's the kind of training we're talking about, you don't have to go out necessarily and purchase anything, some boards of medicine have been very helpful in doing this. But, if it's just you, then you, the provider, you would expect the provider to know essentially how they should be securing the health information. And if it's you and a number of people, they should know things like you don't share passwords, you don't put your password on a sticky note, you use an encrypted device, if you can possible do it; things like that.

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

Right.

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

This is John.

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

Go ahead John.

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

Obviously, you accomplished three separate things that we should include. I'm thinking of a presentation that I saw where there were findings from the OCR audits that were performed this year, and they came up with five categories of things that seemed to be missing on all the audits that were performed. And I'm not going remember all five of them but I remember one was related to authentication or identity management, another one related to disaster recovery. And so I'm wondering whether we should be looking to things like OCR's audit history to determine the things that maybe we should recommend as being things that we would focus on for Stage 3.

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

I like that idea.

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

That's definitely an idea, I mean, but the idea for shining the spotlight on the existing training requirements came from review not of the audit results, but of the actual enforcement actions that have been taken, and the deficiencies that were found as part of that exercise. But one thing we can do, we're not on as tight a timeframe with this, we can explore with the Office for Civil Rights, what are the – sort of try to find out what was in that presentation about the deficiencies, if that would be helpful and people want to have a little bit more time to chew on this.

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

I like that idea a lot. This is Dixie.

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

This is Wes. I like the idea, I think we would – we might get to the point where we want to prioritize among the major deficiencies, because the more spotlights you shine, the less it's really a spotlight.

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

Right.

Paul Egerman – Businessman/Software Entrepreneur

And it seems to me – this is Paul – it seems to me we need to choose one, as we chose one for each of Stage 1 and Stage 2, and the fact that we're talking about this is an indication I think there is a feeling that that was successful, that shining the spotlight on one thing was a valuable thing to do. And training is probably a good area.

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

Yeah.

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

This is John Houston. I agree with that, I just thought it may be informative to have some understanding of what the audits identified as being issues, so we could have an informed decision about what the one or two things maybe we want to focus on.

Joy Pritts, JD – Office of the National Coordinator

Yeah.

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

You mean for evidenced-base regulation, is that right?

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

So, this is ...

Joy Pritts, JD – Office of the National Coordinator

This is Joy, I have a copy of their audit report that I will – let me look at it and I'll tell you the answer in about two minutes, okay?

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

Oh, okay.

Paul Egerman – Businessman/Software Entrepreneur

That sounds great.

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

Hi, this is David Holtzman; can you guys hear me now?

Joy Pritts, JD – Office of the National Coordinator

David can do it.

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

We can hear you.

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

Thank you. Finally.

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

Oh I'll bet you were on – were you accidentally on the public line maybe?

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

I was treated as, well, never mind.

Joy Pritts, JD – Office of the National Coordinator

As the general public is treated, right David?

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

Nothing that I can say is going to help us. So here's what I suggest. The actual audit report is not going to point out specific areas of education that were not addressed. But I can speak generally that education, as were many other issues, were identified, particularly with smaller providers, as being a challenge. Now the caveat is that the training requirement under the privacy rule and the security awareness provisions – I'm sorry, the training requirement under the privacy rule and the security awareness provisions under the security rule are somewhat different in that the take-away from the security rule is sort of a continuous or an occasional training activity that does not have to encompass the entire rule at any one sitting, beyond that first presentation, before giving someone access to the electronic protected health information. As opposed to the training requirement of the privacy rule which requires an initial and then occasional follow on training on the organization's complete privacy policies, to comply with the HIPAA rule.

It becomes particularly more significant as we move into the next year or two as significant changes to the privacy rule and some changes to the breach notification rule come online this fall. So there will be essentially a new cycle of training that will need to take place as organizations update to the new privacy rule requirements. So what I would like to suggest is if you can give me 20 minutes at a future meeting, I would be happy to make an express presentation on our audit findings and that may help you in your discussion and deliberations.

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

I think that would be really helpful David. Could that presentation also include some of the detail on the provisions of the privacy rule and security rule around training and education that you just talked about?

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

Sure.

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

So then, we'll have a really complete picture of all of the areas that we might choose to highlight for Meaningful Use Stage 3, and then I think we'll also be in a better position to sort of finalize that we want to pick one versus multiple ones, potentially added to the two that already exist.

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

Sure.

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

So, does that sound good with – does that work for everyone?

Paul Egerman – Businessman/Software Entrepreneur

Yes.

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

This is David. Just to be devil's advocate. So we're not concerned about that this is duplicative or burdensome, just for the sake of calling attention to something, since they are already obligated to do this. I know we've had this debate many times in the past.

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

Yeah, I mean, that's always something, I think, that we should continue to keep in our minds as we consider what, if anything, we would put in this category. I mean, keep in mind that the meaningful use attestation requirements on privacy and security have always been existing obligations, and shining a spotlight on them. Is it worth continuing to do that, I think, should be a theme that we should continue to push on, even as we con – if we think the answer to that is yes, then what would it be?

Joy Pritts, JD – Office of the National Coordinator

Deven, this is Joy, and I'd like to answer David's question with a little bit of just anecdotal information. I will say from my perspective that, and when I go out in the field, I now hear questions about how small providers need to do a security risk assessment, and never heard that before meaningful use. I think...and we have looked at some of the figures from HIMSS, which I know that they're not ideal surveys necessarily, but they show a dramatic increase in the number of security...people reporting having done security risk assessments in the last year or so. And before that, the number who were reporting having done them was pretty stagnant between 75 – around 75 to 80 percent, and it's gone up over 90 percent. So we at least – it's hard to really measure the impact from the measures that we can see, it looks like it's having an effect, at least with the security risk assessment piece.

Paul Egerman – Businessman/Software Entrepreneur

And that's very helpful Joy. This is Paul. And what that says to me is we're – this kind of recommendation could be also valuable, if we went further than just saying that small group practices had to be trained, if we also provided clarity about what are the topics that should be included in that training. You know, you should be doing mobile devices or, whatever it is, because I think if you did that, if I'm hearing you correctly, people would respond by simply doing the training, and that's a good thing.

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

Well, I too have to play devil's advocate for a moment. We don't specify in the security rule, nor in our guidance, any specific topics that need to be covered. In fact, we encourage covered entities to engage in the training that's reasonable and appropriate for the size, complexity and setting in which they operate. And so I think you'd face a challenge in goal setting or specifying a specific training type, training period or content. And so, I just urge you to keep that in mind as you think this through.

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

Yeah. Yeah, I mean certainly in the – with respect to the other attestation requirements, we've always been very careful not to add any additional components to it, but instead to just shine a spotlight on the existing requirement, that's already in HIPAA.

Paul Egerman – Businessman/Software Entrepreneur

Okay.

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

So let's put a pause on this conversation for now. David, our next meeting is actually – it comes up pretty quickly, May 8. So, it's next Wednesday. If you think you can join us for that, given that the conversation will still be pretty fresh in people's minds, we might be able to take care of this then.

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

Well, if you don't mind using a canned presentation that I'm just going to cut and paste slides into and out of, I'll be happy to do it.

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

David, whatever works for you. That I think will be fine. Again, you might not even need to cover all of the issues, just the parts of the audit report that might be relevant to sort of determining areas that might need some emphasis and then the highlights on training and education requirements, I think should do it.

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

Be happy to do it.

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

Thank you. Okay, so, we'll put a pause on this discussion for now and pick it back up on our next meeting. And now the next several questions, 05, 06, 07 and 08 deal with the issue of audit logs or access logs. One of the things that we did in preparing this straw response was to be very careful to look to existing legal requirements in the HIPAA Security Rule, as the sort of basis for where the policy is on the concept of access logs and audit logs to date. What I'm trying to do is to try to separate how you would consider this set of questions in light of existing Security Rule requirements as divorced from what you might do with those capabilities, potentially in response to the HITECH changes to the accounting of disclosure rule, that's part of the HIPAA privacy rule and still part of a pending rulemaking that the Office for Civil Rights is currently working on.

And one of the reasons why I did that is because I think it is important for us, as a group, to consider what the existing policy requirements are on covered entities today, and to what extent are there sort of additional policies or technical requirements that match up to those existing policy requirements. The other reason why I think it's important to bifurcate that conversation is because I think we need some further guidance from HHS, given that this – that the accounting of disclosure issue is part of a pending rulemaking, as to whether it would be worthwhile for the Tiger Team and the Policy Committee to take those sets of issues on. So, just to sort of let you know why the responses to each of these questions is pretty straightforward, not complicated, it's because I did these presuming that – trying to sort of stick to at least initially what's existing law, until we get some more clear guidance about whether there's a desire for us to take this on for accounting of disclosures, too. And so I just want to pause and do a check in with Joy about whether that makes sense.

Joy Pritts, JD – Office of the National Coordinator

Um, I think it makes sense. David?

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

Yeah, I agree and I have to give the caveat that because this is something that we are in the middle of rulemaking and we've already – and the comment period has closed, my ability to say anything more beyond what was in the proposed rule and what the current rule is, I'm kind of limited. So, I'd appreciate it if you do have questions that they not bring me to the edge of where I cannot go.

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

Okay. Do folks sort of fully understand why – the scenario we're sort of dealing with here? Does anybody have any questions before we move to considering ...?

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

I'm not sure – this is Dixie. I think what you're saying is that we'll consider these only in so far as audit is concerned and not accounting of disclosures?

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

Yes.

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

Okay. Yes, I agree.

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

Yeah, sorry if that wasn't clear.

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

Say that one more time, please. I may – it might be I had misunderstood it.

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

We are considering this next set of issues around certain questions around audit logs and formats and retention in the context of Security Rule requirements regarding managing access to records and technical security, and not with respect to accounting of disclosures, because that's part of a pending rulemaking.

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

Thank you. Thank you.

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

Okay. So, with that ...

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

That said, I don't think the RFC itself did a very good job of separating the two, it munged the two terms together...

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

Well, I think it did, I think there was a desire to see if the conversation could be advanced in that way ...

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

Um hmm.

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

... which I totally understand. But I also don't want to put the Tiger Team through the exercise of working this through from, with a view toward being helpful to accounting of disclosures if there isn't really a vehicle for doing that ...

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

Right.

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

... given that there's a pending rulemaking.

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

Yeah, talk about audit, not accounting for disclosures, of disclosures.

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

So with that in mind, we may actually be able to get through this relatively quickly, then again, there may be issues that I didn't foresee. So, question number 5 I think is where we are, yup, is it feasible to certify the compliance of EHRs based on the prescribed standard, which is ASTM, I understand, for audit logs. And here the straw response is to suggest that the Privacy and Security Workgroup assess the comments to the RFC and address this issue, because I think they're talking about, and the standards folks and experts on certification can tell me if I'm wrong, I think they're talking about the existing audit log standard for certified EHR technology.

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

I agree.

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

Okay.

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

Does this kind of assume that the standard is the right standard and the question is only whether or not it should be certified against, or, I mean, that almost seems to jump over the question of should there be a standard for the audit log.

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

Well, that's a good question. It wasn't one asked in the RFC. I certainly think that any question with respect to certification of EHRs in the privacy and security area is one that the Standards Committee could take up.

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

Well, we already did. David doesn't remember, I guess, but ...

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

No, I was just looking at the ...

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

... used to have – enumerated list of data elements and when we discussed it, we said well it would be better if they could refer to a standard instead of make up their own list.

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

Yeah, I was just looking at slide 24, which says that many of the comments received said that there's not an adequate standard yet. So, we're jumping over those comments, which is, I mean ...

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

We concluded the same thing.

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

The feedback I've heard is that it's not a great standard.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, and David, this is Paul. So there were some comments that say it was not an adequate standard, and those are valuable comments. I mean to me, somebody needs to make a decision whether or not that's correct or not, and Standards Committee should be the place where that would occur.

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

Yeah, I agree. Yeah, I don't think there's a policy issue here, I think this is a standards issue.

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

So I – this is Wes. I think the question is how – the question that we're answering about the use of the ASTM standard. Who put that question, is that a question that derives directly from the RFC or is that a question that we created to – I mean, because David's asking if it's the right question and I'm just wondering, do we have any way to control what the question is?

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

Well it's already been asked in the RFC, Wes.

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

Okay. So the question came from the RFC, all right. Okay. That was my question. Thanks.

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

Yeah, it came directly from the RFC. So, there was a missing question or a corollary question and it's within the purview of the Standards Committee to consider that. I would leave that to the Privacy and Security Workgroup to consider that, but certainly with respect to this question, I think it definitely belongs over in that camp.

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

So, would it be worth noting that there were responses about the adequacy of the standard, it should be, I mean, I'm just trying to point out that the feedback – trying to highlight that it maybe requires some consideration.

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

Yeah, we can add that, that members in discussing this question and considering sort of sending it over across to the Standards Committee, wondered whether there is a corollary question about the adequacy of the standard.

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

Well, I was going to go either a little less or a little further than that and say noting that there were comments about the – in the RFC response, about the adequacy of the standard, as opposed to us debating the adequacy of the standard.

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

That's what – I think that's what Deven said earlier would happen, but let me make sure I understand this right. Deven, I think you said that we, the Standards Committee, will get the same list of public comments that you guys had ...

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

Yeah. I mean, I believe that's the case and I'm just flipping to slide 24, in the backup slides and in fact, it is the case that a majority of comments state that the prescribed standard itself is not feasible. So, that is something that in your review, I think, you'll need to take ...

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

I guess as long as ...

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

... is what I'm trying to say. It's not just for this question, but your understanding is that we will do, on our side, our pass we'll...we've already answered these on our own, but now we'll be looking at the public comments and making a decision similar on the standards side. Is that right?

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

All right, so, maybe rather than talk about our own comments, we could make note that in their review, they will consider the range of public comments, including those on feasibility. I also don't mind noting that people noted that that would be a question worth answering; it's not a recommendation, per se, it's just passing it along. Personally, I certainly don't have a problem with that.

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

Well good, let's go with that.

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

Yeah, okay.

Paul Egerman – Businessman/Software Entrepreneur

Okay...

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

Paul, is that you in the background?

Paul Egerman – Businessman/Software Entrepreneur

Yeah, I just said, and let's move on to the next one.

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

Right, okay. Thank you. Appreciate it. So, the next question, is it appropriate to require attestation by meaningful users that the logs are created and maintained for a specific period of time. So here, there's a policy issue embedded in this arguably, so we've created a straw response for your consideration that the HIPAA security rule certainly does not require audit logs be maintained for a specific period of time, or at least that was my impression. It's good we have David on the speaker line so he can help us work through this. So then consequently, we don't necessarily see a reason to require additional policy specifying a timeframe for purposes of compliance with existing law, and then covered entities would certainly make their own decisions about how long they would keep such logs, based on their own internal policies. And then certainly the Standards Committee could decide whether there are any additional technical requirements that would be needed to meet the needs of these entities.

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

This one I think it's all policy.

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

This ...

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

Okay. Yeah, I mean, well, in – sort of whether there would be a time requirement that we would set above and beyond where existing law is, which my understanding is that it leaves it up to the decision of the covered entities and their risk assessment and their internal processes and procedures for compliance with the rule.

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

I think that's correct. I don't, I wouldn't – I would just answer it from the Tiger Team and I don't think it needs any input from standards.

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

Okay.

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

So Dixie, I think you're suggesting that the rest of the answer pretty well describes it, that we don't want to go beyond HIPAA in this area.

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

Yeah, yeah.

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

All right. Okay, good.

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

Okay. All right, the next one involves whether there's a requirement for a standard format for the log files, in order of EHRs, in order to support analysis of access to health information across multiple EHRs or other clinical systems in a healthcare enterprise. And here's another, I believe that this question was – had accounting of disclosures issues in mind, which is certainly for those of us who know a bit about what was in the proposed rule, I think this question seems to sort of incorporate the concepts of logging access across multiple systems into one report. But since we're going to be answering these questions from the viewpoint of existing security rule requirements, the straw answer is quite simple, that no particular format is required. We can continue to sort of scratch this sort of reference to whether the Privacy and Security Workgroup needs to go into – assess this at all, but current policies don't require any specific format and we don't necessarily see a need to dictate a format to support compliance with existing law.

Paul Egerman – Businessman/Software Entrepreneur

And by format, you're talking about a file format?

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

Yeah, it's, I mean, I'm just sort of reading, it says, is there a requirement for a standard format for the log files?

Paul Egerman – Businessman/Software Entrepreneur

Yeah.

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

This is David. I think the only argument in favor of a standard format might be, at least at a policy level, might be that it would facilitate comparisons across systems, when you're trying to track down inappropriate activity that runs across many different products in a given integrated delivery network, or even in a community. And there has been some discussion that, I think we even heard it in one of our very early Standards Committee testimonies, sessions, where it was difficult to track down inappropriate activity because all the log formats were different, and there wasn't even agreement on time stamps, which we've remedied in Stage 2. But, you could argue that standardizing the format might improve the detectability of abuse. And that would be a policy decision. I'm not sure.

Paul Egerman – Businessman/Software Entrepreneur

David, are you advocating for that or are you just making that observation?

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

I don't have enough experience to know, Paul. I mean I've heard people advocate for it, but, in the real world, I don't know how often they run into a problem. I just don't have enough experience.

Paul Egerman – Businessman/Software Entrepreneur

I mean, my observation would be, the only place where we've actually required any kind of file formats is with information exchange. But just doing analysis, perhaps we're better off just requiring things like time stamps and the requirements at a higher level.

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

Yeah and if ...

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

If you want – if you have a requirement to do across – enterprise wide, an audit trail then it would make sense. But I agree with Deven, there – HIPAA doesn't require that, that's beyond what HIPAA requires.

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

Yeah, this is clearly beyond what HIPAA requires, I wasn't trying to imply that this was HIPAA. This would be ...

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

This is ...

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

David, are we wrong about that – oh, or is that John Houston, I thought it was ...

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

Yeah, this is John. No, yeah, you're right about that and I'll tell you from experience, because we do a lot of this work where I'm at, there is an enormous variation between what's in different vendors audit logs and the likes. So, I think trying to develop a standard is going to be difficult, at least in the short term, and I think it probably distracts from probably more important things.

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

But you don't have any trouble dealing with it relative to some of the other things that you'd like to see dealt with John, is that what I hear you saying?

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

Let's put it this way, we've managed to deal with it successfully, so I personally don't see this as being a huge issue. Yes, it would be nice to have uniformity, but I think that it's something we've been able to work with and we do recognize that each vendor sort of has a different philosophy about how they do things. So, we do need to get vendor cooperation on this front as well, which I think again, distracts from other things.

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

I would point out that if we have uniformity of content, then the format mapping, ad hoc format mapping solutions are more feasible and I think I know a lot of enterprises that have gone pretty far on ad hoc mapping of multiple logs, even without a standard on contents. So, I think everyone would agree that standardization would be ideal, it's a question of prioritization and I think I'm hearing a consensus that it's not a top priority.

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

Agreed.

Paul Egerman – Businessman/Software Entrepreneur

Agreed. I think directionally I think we should make recommendations, but in terms of meaningful use, I think it's probably something that's a low priority.

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

Okay. All right, made note that while there are arguments in favor of standardization in this space, that we don't think it should be a priority for meaningful use, given other important priorities to address. Okay. Last one on audit logs; are there any specifications for audit log file formats that are currently in widespread use to support such applications? This sounds like it might, I mean originally we created a response very similar to the previous question about format not being required by current law. But it occurs to me in reading this that this is sort of a corollary to the previous question, that while it might be desirable to have a standard, and I don't know whether we know if any exist out there, we certainly don't think it's a priority for meaningful use. Does that make sense? How do – how would folks answer this?

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

I would – I agree with you, answer it just like the last one.

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

Okay.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, see the answer of previous question.

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

Yeah. All right. All right, we're to our last area of set of issues on the RFC. And this was a set of questions that were not necessary – were not put forth actually by the Tiger Team, we did not come up with these, they were teed up to be included in the RFC by another body, whether it was ONC, another policy advisory body, I'm not sure. But they deal with the issue of patient consent and they note that there are some privacy laws out there that require...that have detailed requirements for patient consent for sharing certain sensitive health information, and in light of these, the RFC put three specific questions forth on this issue. How can this consent essentially be managed so that these populations that are protected by these additional consent laws don't end up being excluded by health information exchange? How can Meaningful Use improve the capacity of the EHR infrastructure to record consent, limiting disclosure to those who are specifically authorized, manage consent expirations and revocations, communicating forward any limitations and restrictions on redisclosure if that's applicable? And then the third one deals with whether or not there are those – are there existing standards that are mature enough to facilitate the exchange of this type of consent information?

And this was a topic that we – that ended up – we ended up talking about in some of our query recommendations, too. And conversations that we've had both in the Policy Committee and previously within the Tiger Team on the issue of data segmentation or sequestration. And given that we know that there are pilots that ONC has launched, here, I think is the best response, or the straw response, I shouldn't say best, it's up to you guys to decide. The straw response that we've offered which is, we really shouldn't discuss this topic, which by the way was designated for Meaningful Use Stage 4, which is many years from today, or more years from today certainly than Stage 3. That we've deferred further discussion on this issue until we get an update on how these Data Segmentation for Privacy Initiative pilot projects that have begun, that are ongoing, and we need an update on those to see how they're doing. It would be impossible, if not inadvisable, to try to answer these questions, as complicated and difficult as they are, without some information on how ONC's efforts to sort of test some of the technology in this space, how that's going.

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

I would agree.

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

So, you – this is Dixie – do you think all three of these questions have to do with segmentation?

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

Yes, well, many of them do. But certainly what's being tested in these pilots are technical mechanisms to comply with existing privacy laws that create greater authorization requirements.

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

Well, I asked. I think this clearly needs – the obtaining, the management of consent and obtaining consent, we've talked about this before in other meetings, consent in general is a huge issue that needs to be addressed across organizational data exchange, we've made recommendations in that area. I would agree that we shouldn't be – I agree with your response with respect to segmentation, but in general, policy and standards around how to share and manage consents across organization is a big topic.

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

Well it is, and frankly, we already, as part of our query recommendations, the ones already adopted by the Policy Committee, specifically tasked to the Standards Committee, sort of looking into the technical aspects of being able to at least communicate the consents.

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

I think you should capture that very thought in this response.

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

Okay.

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

So that the response isn't just about data segmentation, but also says, we've made recommendations in this area and refer to those recommendations.

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

That makes sense Dixie. Thank you for reminding me about that. Good point. Are there other thoughts?

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

This is David. I have no objections to deferring this one. It's complicated and controversial and I think there's a lot more to be learned before we dive into it.

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

So this is MacKenzie, I just wanted to make everyone aware since the draft agenda hasn't gone out yet for next week's Policy Committee meeting, but Joy will be giving an update on her office's activities and this will be part of that update.

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

Joy Pritts, JD – Office of the National Coordinator
Along with the NSTIC apparently.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director
Joy, you're going to be busy next Tuesday.

Joy Pritts, JD – Office of the National Coordinator
Like any other Tuesday Deven, like any other...

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director
Like any other – oh, okay. All right. Well folks, I will tweak this response accordingly to recognize our previous recommendations on the consent issue, as well as our desire to defer discussion on the issue of data segmentation, pending update on the pilots. And with that, I think we're actually done.

M
Great.

Paul Egerman – Businessman/Software Entrepreneur
Is there a chance for public comment?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director
Yeah, we do. The one thing I will sort of tee up, and we can, since we're close to public comment period anyway. One thing I would like to tee up that we can chat about in addition to the topics that we have David Holtzman tee up to educate us on so we can complete that one question is to sort of consider these two topics, and really which of these two topics that we might turn to next. They're on our agenda for the year, and it's really a matter of sort of prioritizing them and we'll...rather than get into a discussion on this call, since we're wrapping up and we want to leave some time for public comment, we'll pick it up in the next call. But they are cloud computing and right of access in an electronic environment, we two that we're tee up for us. And we can discuss both of those in some more detail, what pieces of that, what we would include, what should be the bigger priority on our next call. Okay, with that, I think we can open to public comment MacKenzie.

Public Comment

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

Great. Operator, can you please open the lines 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're listening via your telephone, you may press *1 at this time to be entered into the queue. We have no comment at this time.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director
Okay, we give you six minutes back.

Paul Egerman – Businessman/Software Entrepreneur
Excellent discussion.

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

Thanks everybody.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director
Thank you everyone.