

**HIT Policy Committee
Privacy and Security Tiger Team
Subgroup Discussion: Meaningful Use 3 RFC
Transcript
July 29, 2013**

Presentation

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Good afternoon, everyone. This is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Policy Privacy and Security Tiger Team. This is a conference call and there will be time for public comment. As a reminder to those speaking, please announce yourself before speaking for the transcript, and I will now take roll call. Deven McGraw?

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

Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Paul Egerman?

Paul Egerman – Businessman/Software Entrepreneur

Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Dave McCallie?

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

We have only—hey, Michelle. We have, it's a subgroup call, so there'll be probably, I think it's fine to go through the roll since we invited everyone to come in, but there'll be probably lots of people who won't be on.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Okay. Thank you, Deven. Dixie Baker?

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

Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Gayle Harrell? John Houston? Judy Faulkner?

Judy Faulkner, MS – Founder & Chief Executive Officer – EPIC Systems Corporation

Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Leslie Francis? Micky Tripathi? Wes Rishel?

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

Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Kitt Winter? And are there any ONC staff members on the line?

Kathryn Marchesini – Office of the National Coordinator

Kathryn Marchesini.

Will Phelps – Office of the National Coordinator

Will Phelps.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thank you, guys. With that, I'll turn it over to Deven.

John Houston – University of Pittsburgh Medical Center

This is John—John Houston is on the phone. I just got in.

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

Great. Thanks, John—and I know we also have Verne Rinker from the Office for Civil Rights on the line. He's filling in as our liaison while David Holtzman is on vacation.

Thank you all for coming onto the call today. This call is our subgroup call, but I'm glad that we have some other Tiger Team members participating on the call as well. Our goal today is to wrap up our discussion on what we're going to recommend for Meaningful Use Stage 3. What we've really been focusing on in our previous calls is trying to think about what, beyond mere attestation we'd use to draw greater attention to the requirement to do a risk assessment, which is both a HIPAA security role requirement but also has been part of Meaningful Use since Stage 1.

We had initially thought about what additional security rule provisions what we might want to shine a spotlight on in Stage 3, but essentially on our calls has been sort of coalescing around the idea that rather than add more provisions to Meaningful Use, we might think about how to make the existing requirements a little more meaningful, for lack of a better word, measured potentially through something beyond attestation, or making that attestation have a little more background to it or oomph. I don't want to say the word "meaningful" again.

What we did, in preparation for this call, we've had a previous call on this issue where we were talking about a number of potential suggestions for doing more than mere attestation for the security risk assessment, and you'll see some straw responses in the next couple of slides, but before I move on, I want to pause and see if, Paul, if you want to add anything before we get started.

Paul Eggerman – Businessman/Software Entrepreneur

Well, I mean, the main issue here is that when we did Stage 1 is where we put in some comments about encryption, and it turns out that there is a belief that what we said there was actually very useful and successful to sort of clarify some things in a lot of people's minds. It was a positive step forward. I think one of the things that made that particularly successful was that it's a very specific recommendation.

I think you'll see that in the subsequent slides that Deven presents. We didn't just say, "Do something about security," we were very specific about addressing encryption of that data at rest and clarifying what that meant to address it. Why don't you go ahead, Deven?

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

Okay, terrific. All right, so here are the suggestions that we are presenting for discussion today and that ultimately, if we get consensus, we would present to the Policy Committee as our recommendation for the third stage of Meaningful Use. CMS should really provide additional education.

For example, through FAQs to the meaningful user community on the expectations and importance of conducting and documenting security risk assessments, and specifically, the FAQs would discuss the availability use benefits of third party assessment tools and services, and a risk assessment checklist, particularly those developed by regulators. The FAQs could also highlight, in particular for larger entities who may be able to afford this, the option or value of having internal auditors leverage OCR's audit plan to conduct substantive preaudits, now that I am reminding myself of this recommendation. *[Laughter]*

The issue for larger entities here, why they're highlighted, is that they often have the staff to do an internal audit to be able to look at what OCR's audit plan was to be able to leverage that in examining their own security risk assessment activities. Such approach is to really provide entities with a higher level of assurance that certification and HIPAA security rule requirements have been met. This is really trying to sort of beef up the amount of information that goes out to the Meaningful User community about both the importance of the security risk assessments, the need to document it, and also for alerting Meaningful Users to a set of tools they can use to make sure that they do it right.

We're also recommending potential accountability measures. For example, identifying the individual or individuals who are responsible for the security risk assessment and even potentially requiring signatures from these individuals.

Then the other idea which we are putting forward is linking attestation to specific Meaningful Use objectives, rather than just presenting it as a single stand-alone measure at the end of the process; specifically, requiring attestation of risk assessment has been performed on any new functionality provided as a result of deploying the 2014 Meaningful Use criteria, which focused on exchange and interoperability between organizations as well as consumer engagement.

Our thoughts are that this approach could increase the likelihood that the risk assessments are performed and focused in particular on these new functionalities. This idea came out of the conversations that I was fortunate to be part of involving a number of Chief Information Security Officers, where one of them suggested that he was not being invited into the room where Meaningful Use preparation was happening because they, you know, discussions around deploying the portal because they sort of saw his activity as being related just to the check the box on the security risk assessment and not to ongoing discussions about how to deploy these new functionalities.

Those are the straw recommendations that we're putting up for your discussion today. It's a combination of greater education to the Meaningful User community as well as trying to think about workable ways to ask people to be more accountable for the risk assignments that they are required to do, and so we're ready to discuss these now. *[Cross talk]* I think it was John, and then I think it was Dixie. *[Laughter]*

John Houston – University of Pittsburgh Medical Center

Yeah. Back to response one, if you want to put the slide back up. I think one of the things that really never comes across clearly in the Meaningful Use, doing the risk assessment—I don't understand if it's implied or it's actually stated in a way that's not real clear—is part of the risk assessment process really requires that an organization complies with it. Now, you put that in your second bullet point. I think that, in my opinion, this needs to be stressed, because a lot of people say, "All I gotta do is do a risk assessment."

So this idea that the risk assessment really, frankly, says, "You've done a risk assessment, you've determined where your gaps are with respect to HIPAA compliance, and you've taken appropriate steps"—because you still have to be HIPAA compliant. I think sometimes that is, that idea is secondary in people's thinking and that really ultimately, at the end of the day, you're certifying not just the risk assessment, but you're certifying in a way the HIPAA compliance.

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

This is Wes. I think John has hit on a great point, and we should definitely include it.

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

Okay. It's a great idea. Include—then the emphasis that essentially, what the risk assessment is designed to do is to assess compliance with HIPAA. Did I get that right, John?

John Houston – University of Pittsburgh Medical Center

No, no. The requirement is not just to do a risk assessment but to take action—

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

Yeah, yeah.

John Houston – University of Pittsburgh Medical Center

- prioritize the action based on the risk assessment and that by Meaningful Use Stage 3, they ought to be able to demonstrate what actions they've taken based on risk assessments and what actions they have planned at the time of attestation. Let's say there's an investigation a year after attestation, either because of an incident or because of auditing. If they can't show that they made progress on the goals they set as part of the risk assessment, then they really have not conformed.

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

This is Dixie. I was gonna comment on the first slide, one of two, that while I think that additional education is important, I don't see it as a Meaningful Use measure. I think what John and Wes just discussed would be a better thing to put on a recommendation for a Meaningful Use measure, is that they would need to document the results of their risk assessment and the actions taken and planned as a result of that risk assessment. I think that would be a Meaningful Use measure.

John Houston – University of Pittsburgh Medical Center

But let me take it one little tiny step further, Dixie—and maybe you implied this—the steps taken to comply with HIPAA, because I think there still is this gap of understanding that the risk assessment ties to gaps that might exist in terms of HIPAA compliance, and you're really supposed to take those gaps and close those gaps, to Wes' point. It all goes, sort of, it's a continuum and risk assessment is sort of a middle phase, but HIPAA compliance is ultimately the end requirement, and it's not ...

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

Yeah, I agree. I think that's right, yeah. The other comment I wanted to make, Deven, is that I remember early on we had our very first conversation about this. I had been told that, by some people that do independent risk assessment, that the number of people who are actually doing risk assessment had seemed to have gone up as a result of that Meaningful Use measure—

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

Yeah.

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

- and somebody referred you to, they gave a name at CMS who had metrics on their audits and you were gonna bring it back to this group. I'd be really interested in seeing what they found, what CMS has found in terms of difference that it actually made in making the risk assessment a Meaningful Use measure. Because if it really is increasing, I would strongly support continuing it to Meaningful Use 3.

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

Well, I don't—so, Dixie, as we learned from Steve Posnack, who's been working with CMS, who's at ONC, I think most of you know Steve—

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

Yeah.

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

- who has been working with CMS on the audits that they've been doing of Meaningful Users, so auditing compliance with Meaningful Use requirements. While we don't have specific metrics, and frankly I don't know if we would be able to get them, what we do know is that, with respect to the privacy and security category, and the attestation of having done the security risk assessment, is that there are a number of entities who have attested to doing the risk assessment—they all do—but that the documentation on those risk assessments is significantly lacking.

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

Okay.

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

It sounds like there needs to be a greater emphasis on the documentation aspect of it than is currently in the recommendation. Now, having said that, I want to do a gut check with you all. Are we telling people that they have to submit that documentation as part of Meaningful Use, or are we instead wording the objective much more strongly on the documentation and HIPAA compliance aspects of it, but still expecting people in their Meaningful Use submissions to essentially agree that they've done this without a proactive requirement to necessarily submit it?

John Houston – University of Pittsburgh Medical Center

I think it's the latter. Just submitting a bunch of documentation to me is a paper chase, but an attestation or a certification saying you've documented it that you can point to in an audit.

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

Right, and the person responsible.

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

Right, and so I think we can definitely word this so that it's much stronger on the documentation point, including that steps have been taken to assure compliance with the HIPAA security rule, and we can get this out to folks to wordsmith offline, but generally, we are still asking for people to attest that in fact they have done this level of work—done the risk assessments, addressed new functionalities, addressed deficiencies, documented all of that, and that is a big part of what they could be audited on.

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

And here's that person that you could call and find out if you—

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

Right, and that gets to identifying the individuals who are responsible for having done it, and the other recommendation that we have which involves attesting not just that you've done it overall, but that you've addressed the specific new functionalities for these specific objectives.

John Houston – University of Pittsburgh Medical Center

Can I suggest that there's actually three contacts? The first is that you have the person or organization that did the risk assessment for the organization; the second is the person that ultimately attests to the accuracy of it; and the third is the custodian of the records, the risk assessment documentation. I know that sounds awful formal, but [*Cross talk*]—

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

Well, in a solo doc practice?

John Houston – University of Pittsburgh Medical Center

It may be one person.

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

Okay.

John Houston – University of Pittsburgh Medical Center

At UPMC, I can tell you, there were two separate organizations within UPMC that were responsible for my risk assessment, there was the person that would be me that would be signing the attestation, and our Audit Department would be the custodian of the record.

Paul Egerman – Businessman/Software Entrepreneur

This is Paul. This is helpful to hear, John, but I'm trying to understand—for the attestation process, why is it important that we identify who those individuals are?

John Houston – University of Pittsburgh Medical Center

I think it just simply goes to the credibility and the fact that you've done it. I mean, you can say—you know, I think the problem is, is that when somebody comes and says, "You're gonna go get audited," I don't want for somebody to go in and say, "Oh geez, I guess we better go do our risk assessment now." To me, it's a no brainer, because I know all of those different groups in my organization that get all of that.

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

Yeah. I think the idea is that the process of identifying the person who's responsible—and it may, in fact, be one person in a small practice—but that that sort of underscores the importance of this measure **and** that it's not just a checked box.

Will Phelps – Office of the National Coordinator

If it's got identification, they'll leave the person possibly susceptible to, like, marketing efforts, and everybody wants to sell security stuff. If you know who the right individual is to contact at an organization—

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

Well, why would that—only if CMS release that information would it be—

Will Phelps – Office of the National Coordinator

Well, could CMS release it?

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

I don't know that they would. It's an internal report that's sent to them.

Paul Eggerman – Businessman/Software Entrepreneur

Historically, I don't think they have released patient information, right? I mean, they've released who has tested, but not what they filed as their—I mean, that's, you can argue that there's some benefit from analytics based on aggregate numbers out of attestation, but to say that this organization did not attest on breast exams or something is pretty sensitive.

John Houston – University of Pittsburgh Medical Center

Well, they have not released who the OCR audited, correct? Are they required to release details about—

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

No.

Will Phelps – Office of the National Coordinator

Well, we're talking here about attestation rather than audits, but I would say, again, I don't think they release the details of audits. I've certainly, all I've ever seen is the published agreements that occur when an action is finalized.

Kathryn Marchesini – Office of the National Coordinator

This is Kathryn from ONC, and I'll just speak to, I guess, the Privacy Act in general. I guess once CMS would get information, federal agencies, they're not necessarily able to disclose information except for interagency, more for a need to know basis, if there's a FOIA request or if it's a routine use, so it's compatible with the purpose for which the information was collected and published by the agency. For any reason, the agency must give notice to the individual, if it was, for example, for one of those purposes.

Will Phelps – Office of the National Coordinator

That's very helpful, thank you. The information could be released as a FOIA request; did I hear that right?

Kathryn Marchesini – Office of the National Coordinator

I can't speak specifically for, I guess, this example. This is a general, kind of the Privacy Act as it applies to federal agencies. In theory, unless there's other laws that particularly would apply, it could be—

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

I don't know. I don't know, Kathryn. Usually down to individual level data is exempted under FOIA, under the Privacy Act.

Will Phelps – Office of the National Coordinator

Well, and Deven, perhaps we're accidentally going too far into a tangential issue. It's basically, my hesitancy about identifying the individuals, to think through if there's any downside to those individuals or to the organization to have that identification occur. That's just a question I'm asking, and if there is none, there's really—anyway, we don't need to spend lots more time talking about it, because it's a distraction from the major issue. The major issue here is, as John has pointed out, the value—John and Wesley pointed out—is a valuable addition that they want to add to this meeting and we should be sure that we do that.

John Houston – University of Pittsburgh Medical Center

Well, does somebody have to attest to Meaningful Use certification overall?

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

Yeah, good question.

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

Yeah.

John Houston – University of Pittsburgh Medical Center

Because if that's the case, it's nothing more than—there really isn't any increased exposure and then you have a second person attesting to something, so I guess the question to ask is, have they had an issue with anybody trying to go after information associated with individuals that the test—if people make Freedom of Information requests for individuals who have attested to Meaningful Use overall.

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

Not that I know of. We will do a double check on that, just to be sure, but I don't believe so.

Will Phelps – Office of the National Coordinator

I think that we, the two takeaways here are calling attention to at least the CISO in the attestation form and—three takeaways. Then, exactly what it says on the second bullet, that requiring risk assessment on new functionality is important. The third takeaway would be requiring attestation about progress made against the—I'm forgetting the word, but for remediation of previously identified issues.

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

Right, addressing deficiencies.

Male

Right.

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

Yep. I think that's right, and certainly providing education on all that is helpful, but it sounds like we want to emphasize the accountability aspects of this first in terms of the sort of order of presenting.

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

Yeah. I think that it's not even—you know, it's supportive of this attestation, this may be needed, additional education may be needed. The Meaningful Users out there are gonna pay attention to what they have to attest to.

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

Yeah, yeah. Agree. Sounds like a good recommendation to me. What I propose, that Paul and I work to incorporate this discussion into these responses so that they better reflect what we want to recommend to the Policy Committee. We'll get it out this week to you all to review with the hope that we can clear up any remaining wordsmithing issues via e-mail and then ideally be able to present this to the Policy Committee at the August meeting in addition to the query recommendations which we finalize. Does that sound good?

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

Yes.

Paul Egerman – Businessman/Software Entrepreneur

Yep.

Will Phelps – Office of the National Coordinator

Yes.

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

All right, terrific. Any other thoughts? We might be able to end this call early.

John Houston – University of Pittsburgh Medical Center

Well, are we allowed to—I mean, this is Meaningful Use Stage 3, correct?

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

That's correct.

John Houston – University of Pittsburgh Medical Center

I guess the question is, is that, do we need to go anywhere past just this notion of risk assessment and attestation or risk assessments? Is there something else that needs to occur with respect to security and Meaningful Use that just goes beyond risk assessment?

The one think I'm thinking of, verbally thinking of is, is there something that needs to be done with respect to business associates or things of that sort? Because to me that's sort of one of the big issues that I see in the industry now is business associate compliance, or is that just simply opening Pandora's box?

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

Well, I think you'd want to think through, John—the business associate issue to me feels like a separate one that, in terms of sort of thinking what you want to use Meaningful Use as a tool to accomplish, especially given that the entity who would be on the hook would be the covered entity in a Meaningful Use objective situation. Whereas I suspect that on the business associate side, we're really eager to see more compliance by the business associates themselves and maybe even ideally better resources for covered entities to choose compliant business associates, but that feels like a really big topic, for which Meaningful Use may not be as great of a *[Cross talk]*.

John Houston – University of Pittsburgh Medical Center

I agree. I was more objectively thinking, is there another topic that we think we feel needs to have an inclusion in this, in addition to *[Cross talk]*.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, and this is Paul. Let me respond to that. As I look at the slides—I think the discussion we just had was great. The question I want to ask is, do we want to also say something very specific? Do you want to say something like, if you want an attestation that a risk assessment was done, do you download transmit function, for example? That's gonna be a new capability in Stage 3 and to use that as a way to shine a spotlight on something or to say that a new attestation, that a risk assessment possibly is done on the use on mobile devices within the institutions, since that seems to be a problem area.

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

I thought we did say we were gonna add the specific exchange and consumer interactions to get additional focus. That's in slide 2 there.

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

Yeah. I thought that's what we said, too.

John Houston – University of Pittsburgh Medical Center

Okay, so we agreed that we are going to do that, then.

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

Yeah.

John Houston – University of Pittsburgh Medical Center

Okay, I'm sorry; I missed that. That's good.

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

It wouldn't hurt in the first one about asking them to attest to risk assessment, to ask them to attest that their business associates have done risk assessment as well.

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

Now, you hold them responsible for that? Are you sure you want to do that?

Will Phelps – Office of the National Coordinator

Yeah. I agree with what Deven just said.

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

Yeah, I do, too. I disagree with me, Deven.

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

[Laughter]

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

[Laughter]

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

It's okay to think out loud.

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

Yeah. [Laughter]

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

All right, well, you all have just done terrific work on this. The one thing that we will ask you to do is to review the text on e-mail when we get it out to you and respond back with any wordsmithing changes that you want to see so that we can get this into the pipeline for discussion at what is starting to look like a very full August Policy Committee meeting. I think there's a lot of other Meaningful Use Stage 3 issues that are gonna be on the agenda, too, in addition to our query recommendation.

John Houston – University of Pittsburgh Medical Center

Is there going to be a, is this going to get fed out, distributed to the larger Tiger Team for review?

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

Yes.

John Houston – University of Pittsburgh Medical Center

Okay. Great. I think that's important.

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

Yeah, absolutely. Okay, I think we're ready for public comment, Michelle.

Public Comment

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Okay. Operator, can you please open the lines?

Ashley Griffin – 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 have no comment at this time.

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

All right, terrific. Thank you all very much. Keep an eye on your e-mail inboxes and everyone have a good rest of your day.

John Houston – University of Pittsburgh Medical Center

Thanks, Deven.

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