

**HIT Policy Committee  
Privacy & Security Tiger Team  
Transcript  
August 19, 2013**

**Presentation**

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

Good afternoon everyone. This is a meeting of the Health IT Policy Privacy & Security Tiger Team and the Data Intermediary Tiger Team as well was invited. This is a public call and there will be time for public comment. Please remember that the call is being transcribed and recorded, so please state your name when speaking. I'll now take roll. 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**

David McCallie?

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

Here.

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

Dixie Baker?

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

I'm here.

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

Gayle Harrell? John Houston?

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

Here.

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

Judy Faulkner?

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

Here.

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

Leslie Francis?

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

Here.

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

Micky Tripathi? Wes Rishel?

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

We know he's here.

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

Yes. Kitt Winter? David Holtzman?

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

OCR staff, David Holtzman, yes.

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

Welcome back David.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Bonjour.

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

Are there any members from the Tiger – the Data Intermediary Tiger Team on?

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Hi, this is Marc Overhage.

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

Anyone else?

**Kathleen Blake, MD, MPH – Vice President, AMA-Convended Physician Consortium for Performance Improvement – American Medical Association**

Kathleen Blake, AMA.

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

Oh, sorry, go ahead.

**Walter Sujansky, MD, PhD – President – Sujansky & Associates**

Ladies first.

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

I heard Kathleen from the AMA.

**Kathleen Blake, MD, MPH – Vice President, AMA-Convended Physician Consortium for Performance Improvement – American Medical Association**

Yes.

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

Yeah.

**Walter Sujansky, MD, PhD – President – Sujansky & Associates**

And this is Walter Sujansky.

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

Are there any ONC staff members on the line?

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

Kathryn Marchesini.

**Kevin Larsen, MD – Medical Director for Meaningful Use – Office of the National Coordinator**

This is Kevin Larsen.

**Jesse C. James, MD, MBA – Office of the National Coordinator**

And Jesse James.

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

Okay, thank you. With that, I'll turn it over to you Deven.

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

Okay. Great. Thank you. We're just going to spend a few minutes at the top of the call giving you all an update on the virtual hearing that we're going to have on the accounting of disclosures issue and then we'll use the bulk of the call to talk about privacy and security issues that may arise with respect to the use of data intermediaries for quality measure calculation and reporting, the data analytics piece on quality. And this is – this presentation will involve an update from the Quality Measures Tiger Team on some conclusions that they reached with respect to the use of data intermediaries for – purposes. And then we will sort of discuss what privacy and security issues arise with respect to using intermediaries for those purposes.

And we'll begin that discussion with a reminder of what we as a Tiger Team and Health IT Policy Committee have already said about the use of intermediaries, and we'll see whether we feel like we already covered it in that recommendation, which we did a long time ago, when we were first formed as a Tiger Team back in the summer of 2010. And we'll have a chance today to sort of think about those recommendations as applied to this particular use case and whether there are any additional issues that we may want to surface. And then we'll move into our customary period of public comment and we'll be done. We have 90 minutes to do all of that today. Paul Egerman, do you have anything to add before...do the –

**Paul Egerman – Businessman/Software Entrepreneur**

As usual Deven, you did a perfect job of summarizing. Are we going to advance the slides to the next thing on accounting of disclosures?

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

Um, yeah, I'm sorry, you were breaking up a little bit on my line – I – sure.

**Paul Egerman – Businessman/Software Entrepreneur**

Sure. In terms of the status update on the virtual hearing on accounting of disclosures – hmm. Everybody still there?

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

And you sound a lot better, I don't know what that was –

**Paul Egerman – Businessman/Software Entrepreneur**

I don't know what that was either, but, sometimes when my kids were younger, I wished I could talk like that.

**M**

That was the locusts.

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, but to – again, as Deven said, we have really two topics, the first one very briefly in terms of the status update on the accounting for disclosures. We have changed the date, hopefully everyone got the notice so that the date is going to be September 30 at 11:45 and it says here that there will be a panel format and this is going to be a very interesting hearing, is what I would say. I think Leslie Francis and people at NCVHS have been very helpful in providing some additional framing questions and concepts to help us, and so some of those people will be joining us hopefully for the hearing, as will people from the Standards Committee Privacy and Security Workgroup. But this is going to be a very interesting process. And I think we also have – we’re starting to draft a series of potential questions that we want to ask the participants and hopefully we will be sending those out to you shortly. So, did I capture all that correctly Deven?

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

You did. You did. You’ll have an opportunity when you get the questions over email to provide some feedback, so, please watch your email for them so that we don’t spend time on calls ideally, wordsmithing questions and we have them prepared sufficiently in advance for the panelists. But yeah, so you did great.

**Paul Egerman – Businessman/Software Entrepreneur**

And there’s just a lot of interest in this issue, so it should be a spirited hearing, and everyone pays attention to those emails. But look at those questions closely when you get them, we need to think this thing through very carefully.

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

This is John Houston, can I, Deven or Paul, do you have any background on where things stand with regards to the proposed rules and why – I mean this hearing and this – I heard they were sort of imminent still, so –

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

No, I would not say they’re imminent John. I mean, the schedule for regulations is not something that we necessarily know about, but we were asked by the Office – or invited by the Office for Civil Rights to have a hearing on this topic, which would hopefully provide helpful input to them as they work on the rule.

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

Okay, thank you. It’s a little confusing trying to think on why we’re doing a hearing at the same time, some people say it’s just about to be released – but, that’s good to hear.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

John, it’s David Holtzman. Let me clear the air.

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

Hey David.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Thanks Deven. The rule is not at any process of development to where we can forecast when it will be finalized or available for publication. And the – we are grateful for the opportunity to work with the Tiger Team and NCVHS to assist us in getting further clarification and information that will help us as we develop a final rule. And thank you Deven for giving me the time to speak.

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

You’re welcome David, I should have handed it over to you in the first place, so – does that answer your question John? David, that was really helpful.

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

Yes, that's great. It helps me a lot.

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

Okay.

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

Deven, just very quickly – this is Leslie. I want to thank all of you from NCVHS for the inclusiveness and I think it's going to be a terrific hearing.

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

Yeah, I do too. Thank you Leslie, we're pleased to have you all, as well as the members of the Privacy and Security Workgroup from Standards, who are able to attend, it's going to be a – this is really the first time we've had three groups doing this, but we've been wildly successful with two. So, I think we'll be triply successful with three. I'm exceedingly optimistic and we are – I agree with Paul, it's going to be very interesting. Okay, so more on that to come, and in the meantime, the work goes on. We're going to turn it over to, I think Marc Overhage, from Siemens, to sort of talk about the work that the Tiger Team for Quality Measurement has been doing on the use of data intermediaries. Is that correct?

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

That's perfect. And are the slides available, if somebody will drive those.

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

Um, yeah. Altarum can drive them or I can drive them or Paul can drive them.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Excellent, it's good to have three drivers, I'm sure we'll go in the right direction. So thanks everyone and Leslie, it's particularly nice to hear your voice from NCVHS days. Hope all is well. So the Data Intermediary Tiger Team spent time this spring and summer trying to work through this issue that's outlined here of what would be the issues around certification criteria for organizations that would serve as data intermediaries for quality reporting functionality. And as on this slide, I think the underlying notion is that an EHR – certified EHR – certified HIT technology would be one thing used to capture the data, and we'll come back and touch on that, and that the data intermediary would perform analytics and then transmit the data to organizations like CMS, who might consume those results. If we can go to the next slide.

And so just to put this in context, this is sort of a pictorial representation to try to get at the – again, some of the data at least, the provider would input into the EHR, the EHR would perform the capture. The data intermediary performs those data analytics on behalf of the providers and reports the clinical quality data. The intermediary would also provide feedback to the providers and that together you sort of deliver the necessary technology. As we'll talk about in a minute, I think during the deliberations the Tiger Team expanded this a bit to suggest that the intermediary may well include data in these measures that come from other sources than the EHR. Next slide.

So, this just reiterates this notion that the data intermediaries or DIs would perform the analytics on behalf of the provider, submit the data to payers, for quality improvement purposes, other kinds of value-based payments and send the information to CMS for quality reporting. And just examples of – there are organizations serving as data intermediaries today, for example for the physician quality reporting system, the qualified clinical data registries and so on. Next slide. So just examples that exist today. So, under HIPAA's Privacy Rule, as you're all familiar with, business associates are defined and those have evolved as a result of HITECH. I don't think there's any need to dwell on that. If you go to the next slide.

So, to the extent that data intermediaries perform data analytics on behalf of the HIPAA covered healthcare providers, it would seem that they fit the definition of business associates and would presumably enter into the same sorts of business associate agreements as other organizations performing functions on behalf of providers, whether they're eligible hospitals or eligible providers. Next slide. Let's see, so the Tiger Team, as we deliberated on this, really took as a starting place, and this may not end up being the right place, but that this really was a fairly simple example and we should – that should build on the existing frameworks rather than inventing something new. And so when it comes to the question of what should HHS or the Secretary require of a data intermediary, in terms of privacy and security, the basic notion that one, they should attest or be prepared to furnish a copy of the Business Associate agreement that gives them the privilege of holding the data that's going to be used. And then second, that they conform to the requirements similar to a typical certified EHR module for quality, for example, would be subject to that there were auditable data privacy and security plan and policies and procedures that would lead to sort of the secure trans – or support the secure transmission of data to an organization like CMS. So this would be – whether this is certification or some kind of actual verification gets into a little bit of what capacity is and so on. Next slide.

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

Okay, now I think Marc you're getting in – yeah, these are our old recommendations.

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, so this is the point where we pause and where we say thank you Marc.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Perfect.

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, so perfect. Great description. Now, just a couple of observations, one is we talked about certification, you used the expression module to talk about how these data intermediaries would work and wanted to sort of clarify, when – what certification actually certifies this software, it doesn't certify an organization?

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Yeah. Correct.

**Paul Egerman – Businessman/Software Entrepreneur**

You could have a software module that performs some quality – produces the quality reports or does some quality things that are required within meaningful use. And that software module might or might not be provided by a service provider –

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Correct.

**Paul Egerman – Businessman/Software Entrepreneur**

– it could be provided by an intermediary, but it could be like a data warehouse and stuff that's on site, for example.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Correct.

**Paul Egerman – Businessman/Software Entrepreneur**

And so, the focus that we have in this discussion though is really on privacy and security and that's entirely what we are focused on and I think we're focused on that mainly because at the – when this was all presented at the Policy Committee meeting, Farzad asked us to look at it. So that's what –

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Yup.

**Paul Egerman – Businessman/Software Entrepreneur**

– that's what we're doing. And so here on this screen is a summary of things that we've said so far about intermediaries. And maybe Deven, do you want to take us through this?

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

Yeah, sure. So, I actually have a question for Marc before we move into this, if he can remain on, and I may not be the only one. Is that okay Marc?

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Certainly.

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

Yeah. So when you talk about sort of, it sounds like what you're recommending in terms of sort of the module – the certification process for the software than an intermediary might provide for quality measurement purposes that we know that the modules are not required to necessarily meet the security criteria that are required of a base EHR. But it looked to me from the slide that you all had at least initially recommended, and maybe the Policy Committee also agreed, I'm having trouble recalling what was decided on that call, that with respect to this particular module – modular approach. For if you're using sort of outside software such as provided by an intermediary to do your quality metrics, that that software should be tested for at least the secure transmission part. Is that right?

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

What the Tiger Team actually recommended to the Policy Committee was that intermediaries would attest to auditable data privacy and security plan, policies and procedures. In other words, the assumption in the recommendation was that at least in the Meaningful Use Stage 3 timeframe, that attestation to those processes would be the best that we could hope for.

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, but be clear, intermediaries don't do any attestation, right? Because there's no attestation as part of the certification process.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

Right. But let me separate, because you're exactly right. There is software, which is certified –

**Paul Egerman – Businessman/Software Entrepreneur**

Right.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

– but then the intermediaries would – the organizations – the recommendation from the Tiger Team was that they would attest to having those privacy and security plan, policies and procedures which were then subject to audit.

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

This is Wes –

**Paul Egerman – Businessman/Software Entrepreneur**

Who are you attesting to I'm confused.

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

Yeah.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

To CMS.

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

This is Wes, right now, there's no –

**Paul Egerman – Businessman/Software Entrepreneur**

CMS isn't going to – isn't certifying the organization and CMS doesn't audit intermediaries, they just – that part is confusing to me.

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

I have a suggestion –

**Jesse C. James, MD, MBA – Office of the National Coordinator**

– so what might help is – this is Jesse. What might help is that you have to appreciate the roles for the data intermediary; they're both software roles and responsibilities described by the Tiger Team and organizational or entity roles. So, there was role of the software or responsibility of the owner of the software to have that software certified, but also the owner, the entity that's responsible for the software also, through the recommendations, would be able to create new measures. And that's not a role that they could be certified for, but a role that they would apply those measures or have a pathway for those measures to be applied to their program. They would attest to the privacy and security, they would describe their relationship with their providers relative to data quality improvement and quality improvement. So, it's – there's both roles for an organization who have relationships with providers and a role for software that fits into our current understanding of how software is certified.

**Paul Egerman – Businessman/Software Entrepreneur**

And let me make a suggestion is, I mean, what you're proposing is a totally new certification process –

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

Paul –

**Paul Egerman – Businessman/Software Entrepreneur**

– and that's not what's in the scope of this group. In other words, so far we've not had certification of an organization or organizations attesting to anything. And so, that's not something I think – I mean, sorry Wes, were you trying to say something here?

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

Yeah, I'd like to when you're done – I'd like to –

**Paul Egerman – Businessman/Software Entrepreneur**

Go ahead.

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

Okay. So right now, I don't know, maybe our friends from CMS can tell me, but I don't know any legislation that enables a process of certifying HIEs or any other kind of data intermediary related to meaningful use. I mean –

**Paul Egerman – Businessman/Software Entrepreneur**

Well that's right.

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

– but, I think there is a way through this. I mean, I think that it is possible that as part of a certification the entity that is getting certified can attest to some of the characteristics of its operation and if that entity is operating a facility, I don't see why they can't attest to the security of a –

**Paul Egerman – Businessman/Software Entrepreneur**

But where it gets complicated Wes is the entity, again the software is what gets certified. So you could have a vendor that certifies the software and the entity doesn't get certified –

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

The software is – I understand that – well –

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

Yeah, I mean –

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

Okay, so we may – I think there's a solution, but it's not – the important thing is though that the only people who can attest in terms of the legal meaning of attest here, as a condition of receiving incentive payments, are the providers.

**Paul Egerman – Businessman/Software Entrepreneur**

That's correct.

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

Yes.

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

So we can make the provider provide the business associate agreement –

**Paul Egerman – Businessman/Software Entrepreneur**

And that relates to the role of the business associate agreement. So we started this conversation I think with Deven asking a question. I'm wondering, Deven, what you think about taking us through these two slides where we talk a little bit about the business associate agreement and –

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

That was actually going to be my suggestion because I think –

**Paul Egerman – Businessman/Software Entrepreneur**

– because we're getting a little ahead of ourselves, I think, right here.

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

I think this goes to the heart of what's the mechanism or mechanisms for enforcing anything beyond certifying the pieces of the software. So I think it's all related to some of the issues that we – previously. So I agree –

**Paul Egerman – Businessman/Software Entrepreneur**

And so – and also just make – sorry to keep on this, but also make the observation these issues exist not just for these quality intermediaries, but for any intermediaries. It may exist for an HIE, for example. But why don't we go ahead and go through these last two slides and then we can talk some more about it.

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

All right. So these next two slides, and apologies in advance for the density of the text, but they come right from the transmittal letter from September 2010, from our initial summer of recommendations that were also on the topic of meaningful choice, and when meaningful choice would be triggered. But a few of you may remember that we got into those discussions about consent thinking about fair information practices and the use of data intermediaries. And there's a whole series of recommendations in that letter about intermediaries, third party service organizations is what we called them, that we should take a look at and see how they apply to this particular use case and what more, if anything, we might want to say, given the passage of time and given this new use case.

Third party service organizations may not collect, use or disclose personally identifiable information for any purpose, and this is a recommendation, for any purpose other than to provide the services specified in the business associate or service agreement with the data provider and any necessary administrative functions or as required by law. And this was a recommendation that we made consistent with the fair information practice principle promoting collection, use and disclosure limitations. Third party service organizations may retain personally identifiable health information only for as long as reasonably necessary to perform the functions specified in the business associate or service agreement with the data provider and necessary administrative functions. Retention policies for personally identifiable health information must be established, clearly disclosed to customers and overseen. Such data must be securely returned or destroyed at the end of the specified retention period according to established NIST standards and conditions set forth in the business associate or service agreement.

With respect to openness and transparency, we recommended that third party service organizations should be obligated to disclose in their business associate or service agreements with their customers how they use and disclose information, including without limitation their use and disclosure of de-identified data, their retention policies and procedures, and their data security practices. Those numbers at the end of the sentence are typographical errors and don't have any relevance to the discussion. It's not a secret code for additional recommendations. I'm not sure what happened there, maybe I leaned on the keyboard.

On the issue of accountability, we recognized that when these third party service organizations have access to personally identifiable health information, they are required to execute and be bound by business associate agreements under the HIPAA. However, it's not clear that those agreements have historically been sufficiently effective in limiting a third party's use or disclosure of identifiable information, or in providing the required transparency. While significant strides have been made to clarify how business associates may access, use and disclose information received from a covered entity, we raised this concern that business associate agreements, by themselves, do not address the full complement of governance issues, including oversight, accountability, and enforcement. And we recommended that the Health IT Policy Committee oversee further work on these governance issues.

So keeping in mind that the timing of this letter was in 2010, around the time that the Governance Work – that the initial Governance Workgroup was being formed, and they're – and in advance of the RFI on governance for the Nationwide Health Information Network. We anticipated that there would be a governance process that might be relied on to enforce and hold entities accountable for some of the recommendations we had made, so that the business associate agreement would not necessarily have to be the sole vehicle for doing that. We now are three years beyond those recommendations and not entirely clear that there will be any additional governance process for enforcement, although this, I think in many ways touches on some of the threads of the conversation we were just having. What within meaningful use or through other vehicles might we be able to rely on to be able to hold entities accountable is one question? And then perhaps an initial question, even before you get to the issue of policy levers to hold – to ensure accountability, did we – is the analysis that we did about the use of third party service organizations or intermediaries and their need to – the need to have associate agreements define very clearly what the uses of the data are and to have retention policies and to be transparent about all uses, even of de-identified, do those still hold? So –

**Paul Egerman – Businessman/Software Entrepreneur**

So those are interesting issues. So first, I want to say, does anybody have any questions for Deven on what she presented as that summary of what we'd said before about business associates and to summarize our previous recommendations?

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

Deven, this is David. Your summary and the recommendations were clear; maybe you could help me with my poor recollection of all the details of HIPAA. Is the business associate part you covered well, but is quality reporting called out for special treatment under HIPAA or is it just one of the examples for a legitimate healthcare operation?

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

I think it's the latter – what you just said David, but I'll make sure that I'm not missing something by asking David Holtzman to help out with this.

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

Hey Deven.

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

Yeah?

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

This is John Houston. There's a clarification that's important in the last question though. Internal quality reporting's one thing, but there are a lot of quality organizations, accrediting organizations that are business associates that have historically been very aggressive about retaining broad rights to data that participants submit. And so there's another facet to that question that's very important.

**J. Marc Overhage, MD, PhD – Chief Medical Informatics Officer – Siemens Healthcare**

This is Marc Overhage, just on that line. One of the topics that came up in the Tiger Team I want to throw into this thinking mix is that in many cases these organizations, data intermediaries, as we discussed them, we imagined might be doing the quality reporting as a secondary activity, not necessarily as the primary activity, which may influence how you want to discuss this.

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

All right, so let me just ask a threshold question of David Holtzman, is it the case that when you contract with an outside entity to do required quality reporting that involves them having access to protected health information, in order for them to do so, is the assumption that they are business associates and need to be bound by a business associate agreement the right assumption?

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Hi Deven. And thank you to John for allowing me an opportunity to look at the rulebook real quick before I had to answer the question. Deven, the short answer is yes, an entity that is contracted to provide services to the covered entity, even if it's for required healthcare quality reporting services, would be the business associate of the covered entity. And in addition, under the new provisions of the rule, they are directly responsible and liable for compliance with all of the security rule and with selected provisions of the privacy rule. And in addition, should that contract or subcontractor have its own business associate to perform certain functions on its behalf, to carry out that role or responsibility to the covered entity, then that subcontractor would be the business associate to the business associate.

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

This is Dixie; I have a question for clarification.

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

Okay.

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

I notice that on the earlier slide that Marc briefed, it didn't mention accountable care organizations. Is an ACO this type of intermediary?

**Paul Egerman – Businessman/Software Entrepreneur**

No, ACO is a covered entity.

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

Huh, I thought they were a business associate of covered entities.

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

Well, if you form – an accountable care organization is a collection of healthcare providers who agree to work together in order to better coordinate care under a risk-based payment arrangement. An ACO could hire another entity to help them do the data analytics, to help them be a better ACO, and if they did that, they would be – that would be a business associate. But an ACO, by becoming an ACO does not deem you to be a business – it depends. The ACO is the provi – organization of providers.

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

It seems like many ACOs operate at least primary care, so, they are covered entities.

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

Yeah.

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

But it's possible that the ACO corporation doesn't, itself, provide care, right, I mean, that's where it would become a business associate of all the covered entities.

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

But they al – almost always

**Paul Egerman – Businessman/Software Entrepreneur**

Wait, I'm a little confused Dixie. How does this discussion about ACOs and covered entities relate to this – what we're trying to discuss here with the data intermediary?

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

Well that's the first thing that came to mind when we talked about an intermediary that does quality reporting, in my mind, that's the main thing that an ACO does.

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

No, they're really talking Dixie – I mean, it's not like an ACO wouldn't do quality reporting, but they're talking about the quality reporting that has to get done as part of meaningful use.

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

Right, I thought – okay. All right.

**Paul Egerman – Businessman/Software Entrepreneur**

Looks like we're back to where we are with this discussion. So we have this concept of these recommendations we've already made about business associates that apply not just to the quality intermediaries, but to any business associate. So it applies to a practice management company, a software company that does cloud computing, it applies to HIEs. So these things all apply to all of these sort of third party service organizations and the one thing that's very – a little bit interesting was the last statement – one of the last statements I think I heard Marc make where he says that this quality activity might be secondary to other services offered by an intermediary. And what's interesting about that is if I heard David Holtzman correctly, there is no issue about patient consent in terms of use of data for the healthcare organizations quality reports, but there may be issues of patient consent if there are other things going on with that data. And so, if you've got organizations that are not making a clear segregation, the quality data from the other data, it seems like it's potentially confusing.

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

Well, I'm not suggesting that it's not, but it sort of – I think the way that we looked at it when we initially took it on, took this question on back almost three years ago, was through the right lens, right. Which is to presume that when you are providing a patient's data to a third party so that they can perform services for you, your ability to utilize that data, to access it, needs to be very clearly delineated –

**Paul Egerman – Businessman/Software Entrepreneur**

You're talking about the third party service organizations.

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

– in the business – really in the business associate agreement, and that gets also down to issues as – in terms of what else can you do with it? How long can you retain it? And how transparent do you need to be with your customers, which in this case are the healthcare providers about even what you do with de-identified data, which isn't regulated under the HIPAA Privacy Rule. So, we laid forth all of this and recognized that that business associate agreement then becomes an incredibly important vehicle for overseeing how data intermediaries or other service organizations that are business associates utilize data. But we expressed some concerns, even way back then that that agreement in and of itself may not be enough, particularly, I recall this, in circumstances where the bargaining power is more on the side of the business associate than the healthcare provider, which may be an issue of resources, size or other factors.

So, I think we came at in the right lens and then – and you know HITECH gives us some help here. And having finalized rules on these provisions also helps where you know that you have a business associate that has to comply with the HIPAA Security Rule and with certain provisions of the Privacy Rule and this business associate agreement, or it can be held directly accountable by the Office for Civil Rights. And those are all protections that are in place, today, that we don't necessarily have to create on our own, because they exist already in terms of our own policy recommendations. But is there more that we need to do here beyond the foundation that's already been led – been laid, excuse me. And it looks like one of the suggestions from the Tiger Team, from the Quality Measures Tiger Team was that the business associate agreement would somehow need to be attested to and either made available upon request or even produced outright. What do we think about that and any other thoughts we have about strengthening accountability for how an intermediary uses data.

**Paul Egerman – Businessman/Software Entrepreneur**

So, comments on –

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

This is Wes. So Deven, I think a general trend I'm getting from you is that for kind of the economic reasons you outlined, and the limitations of what's required under HIPAA, as opposed to what's permitted under HIPAA. You were reflecting a view of the Privacy Tiger Team going back a couple of years that there were opportunities for sharing of patient data that were not in the best interests of having an interoperable healthcare system. If I'm not putting words that are too strong or incorrect in your mouth, then I'm wondering what is our opportunity now to do something that would affect the regulation that – where we could improve things.

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

It's a good question Wes. I remember thinking at the time that we made these recommendations that the strength of the language about how third party organizations and business associates ought to be clearly limited in their business associate agreements to what they can do with data, which is only what's necessary to fulfill the functions that they've agreed to do. And any necessary administrative tasks that go along with those functions, not everything permissible under HIPAA necessarily. And I also was really proud that we at least argue for transparency, even with respect to de-identified data uses.

But I have been hearing anecdotally about business associate arrangements where the business associate essentially declares ownership of the data and extracts agreements to be able to use the data, certainly in de-identified form, for any use to which the business associate might see fit. And I've even seen one – agreements where there was language in there that said, you'll allow us to create limited data sets out of your data, to use them consistent with HIPAA, in ways that we, business associate, determine. And a limited data set, for those of you who are not familiar with the term, is still identifiable health information, although many of the most typical identifiers, like the name, are stripped out.

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

So let's agree, because you certainly know better than I do, that all that's true, all right, that even some providers who in their best interests feel that that's an unwarranted use of their patient data, are effectively forced by some combination of economics and regulation to sign those business associate agreements –

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

Well, in addition, no – unless it goes further, accreditation, which is incredibly important to the hospitals, a lot of hospitals are forced to sign agreements because they need to be accredited for certain –

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

Yeah, so, you could say for economics, regulation and accreditation are forced to sign business associate agreements. I mean I have to think that UPMC has more bargaining power than my family practitioner, but –

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

We don't – we're forced into – all the time.

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

Okay. So suppose that's all true, how can we make a difference? What can we do, if it's only to raise attention to the issue, that's fine? If there are specific regulations pending or anticipated where – or reasonably possible, where we could influence them, that's fine. I just – I'm doing a Paul here, I'm saying, why are we doing this? Where are we going with this?

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

Well and if that's –

**Kathleen Blake, MD, MPH – Vice President, AMA-Convened Physician Consortium for Performance Improvement – American Medical Association**

So, maybe if I could comment. This is Kathy Blake and I've – I have submitted data to one of these intermediaries, actually, to a registry, but the actual entity that has control of the registry is the hospital, which is required to submit that data to CMS in order to have particular procedures covered, under a so-called coverage with evidence development requirement from CMS. The interesting part is there's actually no agreement with me, as an individual. The agreement is between the hospital and it's payment from CMS. But increasingly clinicians are seeing that there is tremendous value in having this data used in a number of different ways. It has been used to identify disparities, variation in care, complications that otherwise might not be appreciated, but can be detected once you have large volumes. And so I would argue that what's important here, and it is an overused term, is transparency, is that people whose data's being released, and I would argue it's the clinicians as well as the patients, should in some way be made aware of the use of that data and at what level of granularity.

**Paul Egerman – Businessman/Software Entrepreneur**

And so there's a number of issues on the table but –

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

Paul, I only want to interrupt you to ask the person who's typing to please put their phone on mute. Thank you.

**Paul Egerman – Businessman/Software Entrepreneur**

And it's a good thing to talk about transparency and the benefits, and Wes has made some valuable comments about where we are right now. But this discussion started with Deven asking this question that one of the previous slides talked about attaching the business associate agreement, as that would be something that I guess the provider or the hospital would do when the attested to meaningful use. And since that was one of the things that's suggested, I just wanted to see – make sure that we talked about that specific issue.

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

Yeah, I think we should Paul and I think it's related to Wes' overarching comment, like, okay, well what do we do. Like what more could we do.

**Paul Egerman – Businessman/Software Entrepreneur**

And so what – and what I would say on that issue, I'll sort of like draw first blood is to say, I don't think attaching the business associate agreement as part of the attestation accomplishes anything, other than adding a bunch more pages to attestation. Because I can't imagine CMS is going to read through the business associate agreement and do anything with it, to say this is a good agreement or bad agreement, is part of giving out the meaningful use money. And providers have to have business associate agreements with other people, besides the – I mean, they have tons of these agreements, right, with all kinds of vendors. And so, it's odd to ask for business associate agreement attached with a single organ – organization because it sort of implies maybe there's something wrong with that organization compared to the others.

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

Right.

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

A question from Leslie. Does the attestation make it a public document when the business associate agreement might not otherwise be a public document? Because that would enable access by consumers.

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

That's a good question Leslie; I don't know the answer to that. I actually don't know if meaningful use attestations are available to the public.

**Paul Egerman – Businessman/Software Entrepreneur**

Last time I asked, the answer I heard was no, they are not. But I'm not clear on that issue.

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

We can try to find out. One other thought that I had – I'm inclined to, at least at this phase, pending an answer to the question we just – that Leslie just posed, to say that filing the business associate agreement is not necessarily – may not get you very far. But I wonder if you would have to attest not only that you have one, but that it met these recommendations, which include – which are very strong on both limitations of use as well as data retention and transparency.

**Paul Egerman – Businessman/Software Entrepreneur**

The only problem I foresee with that is groups like UPMC might have hundreds of these business associate agreements and their legal staff have to read every single one of them, go back through it to see –

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

We would – I mean if anything, you would do it in the limited context of the use of an intermediary for quality measurement purposes, and that would – but that would – through that limitation, while making it potentially more feasible to comply with, it would limit its reach from an accountability standpoint.

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

If we did – it's Dixie, I think that the statement that we made about openness and transparency is the right statement to make. But I think that what we're driving at here is how to – when an entity that's a business associate, whether it be for quality reporting or any other reason, does use data in ways that are unexpected, how can we make that transparency more transparent? How can we make it more public? And I think attestation to meaning – to a meaningful use objective is too limited, because it's only – it would apply to those intermediaries that are doing, and maybe you want to limit it, but they are doing this type of quality reporting. But I think that what we really want to do is to make any kind of violation or – not violation, but any kind of activity that is more than what is expected, how we can make it more visible? Not to be limited to meaningful use, but more broadly to any intermediary that's doing something that a business associate or a consumer might not expect.

**Paul Egerman – Businessman/Software Entrepreneur**

So Dixie, you raise an interesting issue with the – what I'm hearing, tell me if I've got it right, is you don't think any issue with attestation and the business agreement makes sense, we should be focusing more on like transparency and policy kinds of stuff for the BAs.

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

Yeah, just not limit it to this – today's example, yeah.

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

So I – this is Wes. I think, my immediate reaction to what Dixie said was, well, when all you've got is a hammer, you better go find the nail to pound. And –

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

I feel like we have nails, we just don't have any more hammers.

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

– well, no, I mean – it appears to me, we, for example, we're going to die in our strangling metaphors here. But it seems to me that we may have a certain size nail we can pursue, which is a requirement that in order to get incentives or avoid penalties, that a provider or a hospital must attest that its business associate agreements for the associations that are required for preparing meaningful use data have a transparency requirement on their business associate. Now that's not public information, and it's not directly regulatory impactful on the business associate, but most business associates do consider strongly whether their product interferes with their customers, the hospitals or practices getting a meaningful use – impacting the economics of meaningful use for their clients. Other than that, I think we need some assistance on whether there are other nails to pound.

**Paul Egerman – Businessman/Software Entrepreneur**

Okay, so you're suggesting that there be attestation – that the business associate agreement has transparency and that –

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

Is required.

**Paul Eggerman – Businessman/Software Entrepreneur**

– isn't something...with quality intermediaries. So it's business associate agreement, if any, because there may not be one, if any, has transparency provisions.

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

I'm not sure why you say there may not be one.

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

Yeah, I'm not sure why you say that either.

**Paul Eggerman – Businessman/Software Entrepreneur**

Well because maybe the software system – there's no quality intermediary, maybe it has a –

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

Oh right, if they do it all themselves

**Paul Eggerman – Businessman/Software Entrepreneur**

– develop software system and they don't – they do all their stuff themselves; there's no intermediary, so there's no business associate.

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

Yeah, you're right. So they're regulated under HIPAA as a covered entity and we're willing to rely on other levers there. But it is this – what we're trying to do is change this power relationship that causes the intermediaries to be able to get complete agreement that – from the data providers that they can do what they want with the data.

**Paul Eggerman – Businessman/Software Entrepreneur**

So the way that changes it is by requiring –

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

(Indiscernible)

**Paul Eggerman – Businessman/Software Entrepreneur**

– the provider's the one that's doing the attestation, is that correct Wes, in your proposal?

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

Right.

**Paul Eggerman – Businessman/Software Entrepreneur**

So by requiring this provider says, and you need to fix my business associate agreement otherwise –

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

I need you to agree to be transparent and if you don't then of course, you're violating a contract. And these intermediaries would then face a business decision of is it better to become transparent about what we're doing with the data or is it better to force the issue with our providers and then back through the regulatory mechanism.

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

That's the part we need to capture that Wes just said. It's not just we have transparency, but transparency with respect to the uses of the data.

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

Yeah.

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

Right.

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

So we're asking the providers to attest to the transparency and thinking that this will –

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

No, we're asking the providers to attest that they have an agreement calling for transparency.

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

Yeah, agreed.

**Paul Eggerman – Businessman/Software Entrepreneur**

Again, because we'll ask the providers, if they have a business associate with the data intermediary, to attest that that agreement has transparency.

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

That's right.

**Paul Eggerman – Businessman/Software Entrepreneur**

They may not have one; they're not required to have one.

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

That's correct.

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

This is David. I'm sympathetic and encouraged by the direction and the goals or the spirit of that approach. My skeptical self says the definition of transparency will then shift to be the point of argument and the business associate might offer a transparency phrase like, we will use the data as we see fit to improve the patient's health, which might include, in their mind's eye, calling them at dinner to sell them something. In other words, how do you define what transparency is and make it meaningfully powerful – meaningfully relevant?

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Hi, it's David. Can I speak to that concern for a moment?

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

Yes.

**M**

Please.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

So if the covered entity who has very limited permission to market to a patient, if they couldn't do it, they cannot make it any less restrictive on their business associate. So –

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

Yeah, but the calling – was probably a poor example, but I don't think that's the issue. I think the issue is, if you require a provider to attest that they have a business associate agreement that has transparency provisions in it, what do those look like and is it transparent enough to say, we use your data as we see fit to improve patient care, consistent with HIPAA rules. Would that be enough transparency?

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

Let me – this is David. I want to interrupt and just say David Holtzman, thank you for reminding me of that, I had – it had slipped my mind that you can't use a BA to get around your limits on the covered entity. I had forgotten that, so appreciate that reminder. But it was a bad choice. So go ahead and answer Deven's question.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Oh, thanks. So here's my cop out Deven, as you know, the OCR when we set out the business associate requirements, we have specific standards and boilerplate language that must be included in a business associate agreement and we – and HHS does not restrict or in any way control more stringent language that would be included in a BA agreement. The specifications are merely the floor. So if that is a concern to the Tiger Team that it wishes to bring forward in this particular factual use or use case, then certainly it's within its prerogative to do so.

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

Don't we – this is Dixie. Don't we also have to include, not only that you have transparency, but to also that you have imposed restrictions on the business associates use of the data.

**Paul Egerman – Businessman/Software Entrepreneur**

That's a good question Dixie, because I look at this and I think about – I'm looking at the slide and the third thing on the slide says transparency, but the first thing says you can only use it for one purpose.

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

No, it doesn't say for one, it – you have to – it says you can use it for the purposes specified in the business associate agreement. So, in other words, we weren't trying to create single-use business associates, we –

**Paul Egerman – Businessman/Software Entrepreneur**

Well then – what I don't understand is how these issues interrelate. In other words, if you have one and it says in the agreement what you can use the data for, what do you need the transparency for, because it already says in the agreement what the data can be used for.

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

One's identifiable health information and the other – the transparency item in number three was really aimed at de-identified data, which isn't required to be covered – I mean, if you are hiring a business associate to de-identify your data, you need to specify that in the business associate agreement. But what the BA – what the business associate then subsequently does with de-identified data isn't necessarily required to be in the business associate agreement, and David Holtzman, please correct me if I'm wrong. Because the HIPAA Privacy Rule regulates protected health information, de-identified information is not PHI, so it is not – once it gets in the proper de-identified format, and it meets HIPAA standards with respect to being de-identified, it is not regulated. And many of the arrangements that business associates attempt to craft with health data providers have fairly liberal terms with respect to uses of de-identified data. I can't say that universally, I've just seen a few, because the PHI the protected health information that's identifiable is already fairly well regulated under HIPAA, as David Holtzman just pointed out. And you can't use a business associate agreement to expand what a BA could do, but that HIPAA would not allow them to do. It's the de-identified data, the reason why we did bullet number three was specifically to address transparency around uses of de-identified data.

**Paul Egerman – Businessman/Software Entrepreneur**

Okay, so appreciate that clarification. It's helpful. So then, to cycle back, Wes' suggestion is that one thing that we do as it relates to these quality intermediaries is simply make the recommendation that if there is a data intermediary then the provider organization needs to attest that the business associate agreement includes transparency in language. And similar to what David McCallie said, it would probably have to say a few sentences about what it means to include transparency language.

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

With respect to de-identified data.

**Paul Egerman – Businessman/Software Entrepreneur**

With respect to de-identified data.

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

Well, or any data.

**Paul Egerman – Businessman/Software Entrepreneur**

But that's –

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

Or any data –

**Paul Egerman – Businessman/Software Entrepreneur**

That's the proposal, so the question is, do we think that is helpful and responsive to what we should be doing with this circumstance.

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

Umm –

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

Well, I'm not sure I intended to limit Wes' proposal by my clarifying answer to your question Paul. I continue to think that the recommendations that we made about intermediaries back in September, both with respect to identifiable information and de-identified data, was a good, solid set of recommendations.

**Paul Egerman – Businessman/Software Entrepreneur**

Right.

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

What I'm struggling with is how we enforce them, because –

**Paul Egerman – Businessman/Software Entrepreneur**

And so the issue is, does Wes' – some similar – Wes' suggestion or some variation of that, does that help advance like the enforcement, is it like shining the spotlight on it? Is it doing something that advances the privacy aspect of these iss – intermediaries?

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

I mean, that I think is what I'm struggling with, because it's – I – if we're using meaningful use as a tool, we're essentially putting the onus on providers, even though we've already acknowledged that in many circumstances, they're not the ones often with the bargaining power with these BAs. On the other hand, on the theory that requiring the attestation of the providers will force the intermediary to behave in the way that we want them to behave, because their customers will need them to.

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

So, this is Wes. I just want to make clear, I don't think that transparency is the be all and end all, I'm just suggesting that it's an easy first step – an easier first step than actually forcing a change in the business models of large data intermediaries as step one.

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

Yeah.

**Paul Egerman – Businessman/Software Entrepreneur**

Well, it's also one of the few things we have anything to impact, right?

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

Well I think we could say, if we wanted, that they have to sign business associate agreements that restrict uses of the data, I just think our chance of getting that all the way through and then actively enforced is lower and would be higher if we had more transparency about what was going on.

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

This is Leslie. Could I just – that's why I asked the question about what's publically available information because if the – if transparency is just you tell some kind of regulator who's never going to read it, and it isn't something that a consumer could actually get information about, you don't have a lot of transparency. Granted most consumers won't, but there are various representatives of consumers who are interested in those things –

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

Yeah. I mean, my –

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

– that can help bring pressure.

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

Yeah. This is Wes. My proposal was that these intermediaries be required to be transparent publically, just as they have to do now with various privacy issues associated with any website they put up.

**Paul Eggerman – Businessman/Software Entrepreneur**

But you're vehicle for that is through meaningful use attestation.

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

The vehicle is through these agreements and those are – as we know, are not public. So one of these, if you will, entities that's acting as a consumer representative would have difficulty assuring that X, Y, Z firm had business associate agreements that required their doing it and may not – I don't know what their legal standing is in terms of going to court about that, but – so that is a weakness in my proposal.

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

So, this is David. Deven, a question, another naïve HIPAA question. Where does the Notice of Privacy Practice requirements or conventions, if they're not requirements, fit into this space? Could we suggest that these – that this transparent disclosure be included in the Notice of Privacy Practices?

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

Umm, it's the covered entity that must provide a Notice of Privacy Practices to patients, in the case of healthcare providers and beneficiaries or subscribers in the case of a health plan. And usually what's required to be described, and David Holtzman, I'm going to take a stab at this and ask you to bail me out if I get it wrong or if I miss something, is what is permitted to be done with protected health information. It doesn't extend to requiring you necessarily to disclose even all of your actual data practices, although certainly, you can, and it doesn't extend to requiring you to disclose what either you or your business associates do with the de-identified data.

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

Does it require – so it does cover your business associates, but only the permitted uses.

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

Well, but a business associate does not have to provide a Notice of Privacy Practices to a custo – to a patient.

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

I was under the impression that some covered entities rolled up some of their business associate activities into their Notice of Privacy Practice, for example, ePrescribing; I think it's done that way some times.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Hi, it's David. So, once again, the HIPAA Privacy Rule sets a floor for what has to be included in the Notice of Privacy Practices. And you're absolutely right Deven and I'm sorry, I think it's –

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

David.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

– David, thank you – that a covered entity does have to share with the patient that these disclosures are being made, but these disclosures are permitted without the authorization of the patient under healthcare operations, for these quality purposes. And Deven is correct in that business – in that the further used by the business associate is not required to be specifically called out in the Privacy Notice above and beyond the information about that the covered entity uses this information for its quality purposes and healthcare operations. And as far as the require – as far as any required notice by a business associate, that's not at all contemplated by the Privacy Rule and in the example that you used David, if – in those circumstances, that's above and beyond what's required by the Privacy Rule. Not that it's a bad thing, but it's not required.

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

Okay.

**Paul Egerman – Businessman/Software Entrepreneur**

So where are we on this discussion? Wes has made a suggestion, and it seems like it's the only suggestion we have on the table. What were you going to say Deven?

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

Well it seems like the suggestion that we have on the table is an attestation by meaningful users that they have business associate agreements with any data intermediary that they're using to fulfill their quality measurement functions, as required under meaningful use. And that business associate agreement includes provisions that at least are transparent about the uses and disclosures of both identifiable health information and de-identified information. And that that agreement would not be required to affirmatively be produced as part of meaningful use, but you'd have to attest that those provisions are in there and then upon audit, you might be asked to produce it in order to demonstrate that your attestation was accurate. Although, we do – it sounds like there are at least Leslie and maybe some others on the phone who'd like to get further information from ONC and CMS about how much information that's submitted as part of the meaningful use report by a provider seeking reimbursement under that program, is publically disclosed. Because there might be – if the answer is that that information is – can be obtained publically, including potentially through Freedom of Information Act requests, that might be an incentive, I think, for some people to ask that the agreement be provided, even if it's not necessarily reviewed by CMS as part of the meaningful use adjudication process.

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

Deven, just – Deven, a friendly amendment, or at least a friendly question about an amendment. Is there any reason – given that we're reviewing our 2010 rules which were written without specific narrowing to quality reporting, is there any reason why you would include that quality reporting clause in your proposal? Why not all business associates?

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

Umm, I was under the impression that folks thought an attestation with respect to all BAs would be too burdensome –

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, because the concern is, people have to go back and review all the business associate agreements to see if they comply, and possibly some of them relating to like transparency, this issue may not –

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

Yeah.

**Paul Egerman – Businessman/Software Entrepreneur**

– it may not be important or relevant, depending on what the business associate agreement is, but I was just concerned about some legal department going into overdrive.

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

Is John still on, John Houston, what do you think about that?

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

I am. I sort of missed the last part of what – said. Could you say it again Paul?

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, I'm just concerned that if we say all business associates, an organization like UPMC, in order to attest, the lawyers are going to want to review every single business associate, and you might have tons of them.

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

We do have tons of them and I think, I would agree with you to keep it to a limited subset. The business – by the way, I think the dirty little secret here is a business associate agreements is very difficult to manage, for any size organization. Small hospitals have hundreds of them, large organizations have got thousands of them and it's very difficult to effectively manage that whole process. That's sort of part of the difficulty in all this.

**Paul Egerman – Businessman/Software Entrepreneur**

It's difficult from a vendor's standpoint also.

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

Absolutely.

**Paul Egerman – Businessman/Software Entrepreneur**

Let me just tell you.

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

Well, I me – because I think a lot of times the business model for some of these – is at least partially built on a potential revenue – from the use of de-identified data and you don't want to have to renegotiate these agreements, ideally, with every single customer. You want to have a standard agreement that everybody signs, right? I mean I'm sort of cognizant that this sort of a hornet's nest of issues, but I find the idea of transparency very appealing, it's something that I liked a lot when we came up with these recommendations back in September. It's just trying to figure out a way to shine a spotlight on it, which I think Paul's right to put in those terms, using the policy tools that we have is really, I think it's a challenge.

**Paul Egerman – Businessman/Software Entrepreneur**

So –

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

This is John Houston again. I understand Deven, I understand your point. It's equally – I just personally have found it offensive over the years, I being told in order to stay in business, I need to be accredited and if I want to be accredited I have to agree to these terms. And oh by the way, these terms require me to allow the business associate the – use agreement and to slide the data and agree then – and do all sorts of other things unrelated to the accreditation. Transparency's great, but I still personally find it offensive what I'm forced to sign on to.

**Paul Egerman – Businessman/Software Entrepreneur**

So John, you're sort of saying, this doesn't help you. This is nice thing, but it doesn't really get to the guts of the issue. Is that what I'm hearing?

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

Yeah, that's correct. That's correct. And also –

**Paul Egerman – Businessman/Software Entrepreneur**

It sort of feels like to me like we've got an interesting proposal, but there's not a lot of enthusiasm for it.

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

So should I submit a friendly withdrawal?

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

– I'm going to say, some of this just requires clarification. I'll give you an example, data use agreement. It says in HIPAA that data use agreements have to be signed by the covered entity and the organization that's going to be using the data for research purposes. By putting in a business associate agreement that says that the business associate can use this data, the data under a data use agreement, in my opinion, runs afoul with HIPAA because HIPAA says that the covered entity must sign the data use agreement, not the business associate. So clarification in certain cases may be helpful in trying to prevent some of these unintended uses.

**Paul Egerman – Businessman/Software Entrepreneur**

So I'm not clear John, what are you recommending that we do, I'm talking about the quality intermediaries, what should we be doing, do you think?

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

Personally I think they should be strictly held to what they're – the purposes of the underlying agreement is and they shouldn't be able to use the data for unrelated uses, which is what they're trying to do in a lot of cases.

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

Which is essentially what we said in the recommendations one and two, I'm calling them one and two, the first bullet and the second bullet on this slide that we're looking at.

**Paul Egerman – Businessman/Software Entrepreneur**

But how do we do that is –

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

(indiscernible)

**Paul Egerman – Businessman/Software Entrepreneur**

That's the fundamental issue. The fundamental issue is all we've got is like meaningful use attestation, we can't do anything else, right? We don't have any other policy lever.

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

Yeah, you know, I wonder if it's worth even just reporting on this discussion and resurfacing the recommendations that we initially made.

**Paul Egerman – Businessman/Software Entrepreneur**

I think it could be. I mean the question I also have, it's just a curiosity question if David Holtzman is still on the phone, which is, and does OCR have the ability to audit an intermediary to see what they're doing?

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

Yeah, as a business associate they do because they have direct rights to go after business associates.

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

Yeah, but it would have to be – they would audit them based on the terms of the agreement and whatever sort of legal provisions they have to comply under HIPAA. So that – the Security Rule as David mentioned and some of the Privacy Rule, and then of course, whatever their business associate agreements say, but that's where the sort bargaining power issue comes in.

**Paul Egerman – Businessman/Software Entrepreneur**

Has it ever occurred?

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Well, it's not yet – we're not in the compliance period yet, so the Rules aren't actually being enforced until September 23, so I get to say, no it hasn't occurred because it's not in effect. But let me, once again, take the opportunity to clear the air a little bit. So the enforcement rule provisions that currently apply to covered entities will also comply to business associates. So the Department can initiate investigations or compliance reviews of business associates to determine if they are in compliance with the appropriate provisions of the Security Rule and the Privacy Rules provisions, as they relate to how they're spelled out – I'm sorry, specified in the business associate agreement. As far as the issue of audit, that's a slightly different approach. The Department is, specifically OCR, is evaluating how we'll implement its audit program going forward. So, it wouldn't be – I could not say with any specificity how that's going to be implemented, specifically to this business associate or any business associate.

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

This is Dixie. David, if they – if a covered entity used de-identified data for a purpose that wa – for any purpose, that would be in compliance with HIPAA. If you were – I know you said you aren't auditing –

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

Dixie, I have to stop – Dixie, I'm so sorry, I have to stop you there. So if a covered entity de-identifies data –

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

Uh huh.

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

– that data is no longer subject to the requirements of the Privacy Rule, once the elemen – the 18 data elements have been stripped out or there's been a certification by an appropriate statistician, for example. So already it's removed from the provisions of the Privacy and Security Rule.

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

But that's what we're talking about here, except we have an intermediary who de-identifies the data and if they used it, however, that would be allowed as well, right?

**David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights**

If the business associate agreement provided or permitted the business associate to aggregate data and – which could be – take many forms, and if it resulted in de-identification, then that data would no longer be subject to the requirements of the Rules, beyond – the provisions of the Privacy and Security Rule. However, the data that was originally transmitted to the intermediary would either have to be destroyed or returned to the covered entity or the prime contractor, in the case of a subcontractor, upon the expiration or termination of the business associate agreement.

**Paul Egerman – Businessman/Software Entrepreneur**

Yeah, that's helpful. I'm looking at the clock Deven. I think we're supposed to –

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

I'm looking at the clock, too. One of the things that we'll do, we have another – since we're no longer trying to have the virtual hearing on accounting of disclosures on the sixth of September, we actually do still have a shorter call on that day that we can work to create some language around applying the recommendations that we did in 2010 to this particular circumstance and reflecting some of the poli – the potential approaches that we discussed, but ultimately feel probably won't work. And sort of be writing it up as sort of a reinforcement of our previous recommendations on intermediaries, but an acknowledgement that we lack good tools for enforcing them, just so folks can – we'll have another chance to chew on them. And in the meantime, we can also get an answer to that question about what's publically available in terms of what gets submitted for meaningful use attestation. Does that make sense?

**Paul Egerman – Businessman/Software Entrepreneur**

It does. And so basically we would be reiterating our prior recommendations and summarizing our conversation from today.

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

Yup.

**Paul Egerman – Businessman/Software Entrepreneur**

And I do think that is a good thing to be doing.

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

Sorry, this is Michelle. Sorry Deven, we have decided not to have any meetings on that day, on September 6 –

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

Oh, oh, that's right, so sorry. Don't have a call on the 6<sup>th</sup>.

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

– another call.

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

Yeah.

**Paul Egerman – Businessman/Software Entrepreneur**

So, we'll –

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

So maybe we can try to do some of it in advance by email, but we'll be able to consider what – how we present this to the Policy Committee on another call.

**Paul Egerman – Businessman/Software Entrepreneur**

Right, but we do want to wrap it up before the September 30<sup>th</sup> hearing, because it's hard to do two things at once.

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

I know we need to do that.

**Paul Egerman – Businessman/Software Entrepreneur**

And the 30<sup>th</sup> is a very meaty, challenging topic and we want to make sure that we focus on it 100 percent.

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

Yes.

**Paul Egerman – Businessman/Software Entrepreneur**

So this has been a terrific conversation though, and very helpful, a little troubling, but that's also very helpful. Do we want to open up for public comment and see if there's any public comment.

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

Yes. Thanks Paul.

**Public Comment**

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

Operator, can you please open the lines?

**Caitlin Collins – Altarum Institute**

If you are on the phone and would like to make a public comment please press \*1 at this time. If you are listening via your computer speakers you may dial 1-877-705-2976 and press \*1 to be placed in the comment queue. And we do have a public comment.

**Kelly Cronin, MPH – Health Care Reform Coordinator – Office of the National Coordinator**

This is Kelly Cronin from ONC, I was muted and I couldn't speak earlier. I just wanted to answer Paul's question about what other levers are there and the Medicare Physician Fee Schedule, the last NPRM that came out over the summer did propose some initial thinking about the qualification of clinical data registries under the Physician Quality Reporting Systems. So it's not just the provider attestation under meaningful use that is relevant. It's actually the qualification process that CMS would establish for these registries that could, I think as proposed, they're clarifying that they would be business associates, but there, I guess, would potentially be the opportunity for CMS to follow up with auditing or maybe in coordination with OCR.

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

Kelly, thanks for that point. We'll track that down in advance of our next call as well. That's helpful.

**Paul Egerman – Businessman/Software Entrepreneur**

So we can learn a little bit more about that, that's very helpful.

**Caitlin Collins – Altarum Institute**

We have no more comment at this time.

**Paul Egerman – Businessman/Software Entrepreneur**

Okay, and let me also just take a minute before we end by thanking everyone, especially want to thank our friends at OCR and David Holtzman for being, always very beneficial to have the answers to every question when ask them, so that's terrific. And Marc Overhage and the people in the Data Intermediary Tiger Team for putting together the material. And of course, everybody else. Thank you very much.

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

Thanks everybody.