

**HIT Policy Committee
Privacy & Security Tiger Team
Transcript
December 2, 2013**

Presentation

Christianne Williams – Business Analyst – Office of the National Coordinator

Thank you very much. Good afternoon, this is Christianne Williams with the Office of the National Coordinator. This is a meeting of the Health IT Policy Committee's Privacy & Security Tiger Team. This is a public call and there will be time for public comment at the end of the call. Please remember to state your name before speaking as this meeting is being transcribed and recorded. I will now take roll. Deven McGraw?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

Paul Egerman?

Paul Egerman – Businessman/Software Entrepreneur

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

Dixie Baker?

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

I'm here.

Christianne Williams – Business Analyst – Office of the National Coordinator

Judith Faulkner?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

Leslie Francis? Larry Garber? Gayle Harrell?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

John Houston?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

David McCallie?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

Wes Rishel?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

Micky Tripathi? Kitt Winter?

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

Here.

Christianne Williams – Business Analyst – Office of the National Coordinator

And is there anyone from ONC staff on the line?

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

Kathryn Marchesini.

Christianne Williams – Business Analyst – Office of the National Coordinator

All right, thank you. Is there anyone else? All right, Deven and Paul, I now turn it to you.

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

All right, terrific. Thanks everyone. I hope everybody had a great Thanksgiving. Please remember, when you're not speaking to mute your lines – feedback. What we're going to do today is to finalize recommendations on accounting for disclosures, and we're going to focus in particular on the language around the follow the data approach, which actually begins on slide 6. And there's some other language regarding our recommendations with respect to security rule audit trails that we will also talk about. But otherwise, we are aiming to finalize these recommendations on our call today, so that we can present them to the Health IT Policy Committee at the meeting that's scheduled for Wednesday. And now we have a 24-hour rule with respect to Policy Committee and working group materials, so we will need to get them our slide deck for this presentation by the end of the day today.

So, I'm going to turn it over to Paul in a minute to start leading us through the conversation – the language that begins on slide 6, which is the follow the data approach. But we also did send you a deck with some redline language, tweaking some of our previous recommendations for you to review offline. We're not going to go through those slides today, consistent with our approach of not wordsmithing on the phone, to the extent possible. But we did want to see if anybody, before we dive into the follow the data and audit trail language, we did want to take this opportunity in the very beginning of the call to see if anybody had any questions or concerns about any other language that was in the slide deck? Okay, terrific. Paul, I'm handing it over to you to get us on to follow the data.

Paul Egerman – Businessman/Software Entrepreneur

Great. Thank you very much Deven. So on the screen I switched to slide number 6, which says on it, as the title, Recommendations, Right to a Report of External Disclosures (3 of 7). And what we want to do here is to talk just a minute to make sure there's understanding and a consensus about this thing that we call follow the data approach, and then we have like three slides of examples. I think at the last call David McCallie requested some examples. But the basic concept I want to explain of follow the data is, what we're trying to do with this is to sort of say, well let's think about the entire discussion that we had before about disclosures and this thing called an access report. And to sort of realize that where we ran into difficulties with the accounting of disclosures was around the definition of disclosures, especially around the definition of what constituted a disclosure that involved like employment status of an individual, whether or not they're employed by the facility. That was a difficult topic – trying to find the right word, a difficult topic.

So we say – what we're trying to say with follow the data is to say, instead of thinking about these terms like what is the definition of a disclosure and what is – what are the HIPAA terms. Let's start by thinking about the data itself and what happens to the data and then use that understanding of what happens to the data to determine what are what we would call the type of disclosures that would be included on an accounting of disclosure report. So that's the concept is to sort of follow the data as opposed to trying to get hung up about the definitions. And then what we are saying here, in the red characters, as you see that on the screen, we're trying to show you what changed from last time, so you can see the changes.

The follow the data approach we're saying, should be used to help HHS make this decision about which disclosures should be on the accounting of disclosures report. And the two bullets we have here are first is when the provider sends a copy of the data, and we – I know there's been a few people who have given us some wordsmithing suggestions. But when it goes basically from the EHR to someplace outside of the compliance environment, and that's the compliance environment of the entity or the OCHA. And then the receiving organization could potentially disclose that data themselves, so it's sort of like this concept of a loss of control. And when that occurs, the recipient should be simply listed on the accounting of disclosure report, again, it's just being listed on the report is what happens. So that's like the first bullet. The second bullet basically relates to business associates and it basically says, well, the business associates are able to do the same thing. If they're able to re-disclose the data, if it's outside of the compliance environment of the entity, then the business associate needs to be included on the accounting of disclosures report.

So that's like the definition, and then responding to what David McCallie said, we tried to put together some examples. And here are the examples, I'm going to go through the examples and I'm going to pause to give people a chance to react. So, and again, these are all in red because this is new material that we did not present last time – previously. So the bullets are first data is moved from a provider entity or provider organization to an HIE organization where the HIE is able somehow to control the use and disclosure. Another bullet is if the data is sent to an organization that facilitates ePrescribing, so we didn't really want to name an organization, but I think people know the name of the one we're probably thinking of. Data is sent to a health plan, an insurance company, for payment, or is sent to an external provider, another covered entity, for treatment. Those are all examples that would be listed on a disclosure report. Or our data is sent to a registry for quality improvement that would also be an example of something that would be sent. The idea being all these examples, patients would be informed of where their data is, and we have a right to know.

Here are more examples that help understand the concept of control. If the recipient of the data is able to resell or otherwise monetize the data, that would also be a situation that would be outside the control of the provider and should be – at least the entity would be listed on the report. If the recipient is able to disclose the data to other covered entities. If the recipient is able to use that data somehow for their internal purposes or to create a limited data set or de-identify the data. So those are all examples of what would trigger this concept of leaving the compliance environment and leaving control.

Here are some examples that do not trigger this disclosure report. So the first one is if what happens is you allow a community physician who is not employed by the say hospital, to have a user name or password or whatever other credentials might be used to gain access like any other user, then that's not a type of disclosure that would need to be included on the report. It would, however, be included on the internal investigation responsibilities that we're going to talk about in a minute. And also any automatic transfers of information from an EHR to some other electronic system that may exist within the entity or OHCA. So if there is some other machine or perhaps another computer system that is sending or receiving data to and from the EHR system, that's within the OHCA or the covered entity, that does not have to be included on the accounting of disclosures. Again, the whole concept of trying to simplify this and hopefully make it possibly more useable to patients. So having gone through the example and the explanation let me pause and see what reactions the Tiger Team members have.

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

This is John –

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

Paul, this is David.

Paul Egerman – Businessman/Software Entrepreneur

Go ahead David.

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

It's a good list of examples. I wonder if we should consider including the use cases under Meaningful Use Stage 2 where data expressly leaves the provider's organization, such as the transition of care or use of Direct. Would those be worthwhile listing, simply because that's the purview that we're in?

Paul Egerman – Businessman/Software Entrepreneur

Well if you think so and other people think so, then – I mean, the purpose of listing it is to make sure people understand what we're talking about, and so I think that could be useful and would make sense.

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

Thanks.

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

This is John –

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

Paul, this is Dixie. I have two questions Paul. The first may be related to the fact that I unfortunately had to miss the last meeting, but I don't understand what is meant by outside the compliance environment. Have we defined compliance environment, and I give you as an example on slide 9, access to a hospital EHR by a community physician, a community physician, to me, they're compliance environment is their own practice, not the hospital. And to me the hospital would be outside their compliance environment. So I don't quite understand that term, as we're defining it here.

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

Well, so Dixie, it's Deven. So what we're trying to do is to create an understanding of what's meant by an external disclosure and when does something go really sort of external to an entity. And when we were on our last call we picked up on the term compliance environment for the sort of entity whose disclosure is being considered. And in that example Dixie, it's the hospital's EHR –

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

Oh, okay.

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

– that we're considering whether or not a disclosure has occurred, so it's their compliance environment that that community physician would be within, because they've been issued credentials –

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

I see.

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

– not the community physician. And the concept actually comes – we're borrowing it from a recommendation that we had made previously about what constitutes remote access that would trigger greater authentication requirements, remember, level 2 remote access, remote being beyond the compliance environment. So we're talking about, in that particular example, the hospital and what it has control over and what it needs to protect under the HIPAA security rule for example. And within that environment, arguably things that happen within the boundary are not external and things that go beyond it are; it was just a simple way of trying to conceptualize what's external and what's not.

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

This is Wes.

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

Well I think we should define that Deven, because I didn't, I really didn't get that notion. To me the doctor would be operating within his own or her own compliance environment.

Paul Egerman – Businessman/Software Entrepreneur

Yes, it's the compliance environment of the data. I mean, the fact that the institution –

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

Um hmm.

Paul Egerman – Businessman/Software Entrepreneur

– is the one that is able to give the credentials to the physician.

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

Right, I can understand what you're saying, but I didn't. So I –

Paul Egerman – Businessman/Software Entrepreneur

The institution presumably had a reason to do that, but they have to make a determination that that physician can be trusted and they have some set of rules that that physician has to follow to access the data. And they may also make a determination of what data that physician is able to access, it may not give him access to everything, may not give him access to –

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

Yeah.

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

This is –

Paul Egerman – Businessman/Software Entrepreneur

– they may not have the ability to like post a payment or write-off an account. And so that's all operating within their compliance environment, the compliance environment of the data. So maybe that's not expressed clearly, but that's what it's intended to be.

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

Yeah, I understand, Deven – I understand Deven's explanation, I just think we should – if I didn't understand it, chances are others won't either, so we should articulate that, I think. In terms of the data, who owns the data –

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

This is John Houston, though. This is John Houston.

Paul Egerman – Businessman/Software Entrepreneur

I'm sorry John, you broke up, could you please repeat what you just said.

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

Sure. I – there are still some nuances here that I think are incredibly important and I think that a physician that is on a medical staff of a hospital, typically yes, they're going to be given access to electronic health record system. As much because of the fact – because they're on the medical staff and in order for them to treat a patient that is within the facility in which they're on the medical staff. They need to have access in order for that facility to be able to effectively treat the patient, efficiently treat the patient in order to support that organizations billing and whatever else.

That's a different reality than if you say, okay, I want to give a physician access to an electronic health record and that physician is sitting within his or her own office and maybe potentially having their staff access that medical record as well, of that hospital, that provider, from within the physician practice or physician office setting. One, I would argue is a disclosure, the other one I would argue almost amounts to what I would say is either access by a workforce member. I mean again, the medical sta – being on the medical staff sort of almost extends that physicians relationship to that point, or at least they're part of what you might infer could even be an OHCA. But there really are different – I mean philosophically they're different once you extend to that physician access within a practice.

Paul Egerman – Businessman/Software Entrepreneur

Yes John, this is Paul. They may be different although from a computer – standpoint, very difficult to figure out the difference, where somebody is accessing the data and this kind of information. The distinction between a community physician and a staff physician and certainly the concept employment status is nearly impossible to figure out, based on where things are right now. And the example you gave of the community may let their staff have access to the data, well that’s eyebrow raising, because it depends on how that might occur. But normally, you provide a user name and a password to an individual and do you not let that individual give their credentials to anybody else. And if you have a situation where somehow other members of that community physician’s staff have access, and the physician can control that, then you have sort of left the compliance environment, and that might be a different situation.

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

But, I’m just –

Paul Egerman – Businessman/Software Entrepreneur

But if you leave that co – and you’re right, these things are not simple, there are a lot of nuances to getting this all straight. If you leave that situation aside for a moment, it’s still the organizations decision to give that community physician some level of access and one can think of ways, the reasons that that happen. You have like a cardiologist, and a lot of the patients are at a particular hospital, they might just give the cardiologist access to see what’s going on, but that might be good reason to do that. And whether or not the cardiologist has staff privileges, they might, they can be operating in multiple roles. They may have been the admitting physician, but they also may be just a – they may be going back and looking at the record after the patient’s discharged because they’re trying to figure out something and they’re curious about what really happened.

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

Well I understand that, I’m just – there’s a lot of nuances here that actually do make this compliance ar – this compliance – zone of compliance, zone of whatever less clear than we might think.

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

Well I mean, John, this is Deven. I’m happy to try to provide more clarifying language if you think it would be – again, we’re trying to provide some guidance to HHS about how they can sort of pick this up and implement it, so I don’t know that we have to answer every single permutation –

Paul Egerman – Businessman/Software Entrepreneur

Yeah.

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

– of this. But having said that, what – if people have a better conception of what constitutes an external disclosure in the way that we sort of visualize it when we think about following the data and it moves from one organization and goes outside to another separate organization, compliance environment was the concept that we came up with. But if that’s not – and we can define it, Dixie, I think you raise an important point and we can do that. But if it’s – and it’s not a perfect concept, if there’s a better one, let’s see if we can come up with one, but it’s – we may actually just have to settle for describing it as best we can and let them figure out some of these details in the pilots and implementation.

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

So Deven, this is David. I’m looking back at the previous slide on there, definition of follow the data, and I think you’ve captured the essence of it there pretty well in that it’s when the data itself is transferred to an environment where it’s under different controls. And so if the community physician looks at the data in the hospital’s EHR in some authorized role where he has a right to see that data for the management of the patient, but doesn’t change the control of that data, then that’s not a disclosure. If he downloads it into his own EHR, that is a disclosure because now he has control of it under a different compliance environment. So I like the language that we started with, maybe we just need to flesh it out.

Paul Egerman – Businessman/Software Entrepreneur

Yeah. And so that – .

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

This is Wes.

Paul Egerman – Businessman/Software Entrepreneur

That's how we'll – before you talk Wes, I just wanted to cycle back to John's comment. And one way I interpret what John Houston is saying is, whenever you do something like this, it's – there's always some like boundary conditions or something that exists at the edge that doesn't quite exactly fit the definition and that's probably true. We also want to put this in the context of some of the early slides that we can show is, we're trying to take a situation where we have this concept of an access report and the situation that was kind of unworkable, and come up with something that's workable. And also this is like an initial starting point that we can build on. And so this is not necessarily like either the final word on the thing, it's sort of like a definition of what's inside the organization and what's outside, to be used to help determine what's –

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

But it –

Paul Egerman – Businessman/Software Entrepreneur

– going to be included on the report. Furthermore, you can always – the institution can always do more than what is listed here, in other words –

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

And this is John Houston and I think as we build exchanges and we have better capability to offer more structure – transference of data whether it be through a HIE or through Direct or whatever, this – what I described in large measure goes away. But –

Paul Egerman – Businessman/Software Entrepreneur

That's correct.

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

– in the interim, this is a very prevalent practice of physician practices and physicians in their office looking up records, and I think it does – I'm not sure I agree with David that until they download the record it becomes a disclosure.

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

Well, it's a –

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

This is Wes –

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

...a transfer of –

Paul Egerman – Businessman/Software Entrepreneur

Okay, go ahead Wes.

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

Um, so I think frankly we're violently agreeing with each other here. There's – the issue is what is practical to measure and regulate as opposed to whether the possibility that a physician who is in a work environment with people who are not at all related to the hospital, because they're in his practice, possibility that he sees the data is – clearly creates the possibility that he's obligated to make sure his employees don't misuse the data. But I just – I think we're trying to find something that can be measured and implemented as opposed to the ideal situation. I'd like to actually address, if you could move to the last of the example slides again.

Paul Egerman – Businessman/Software Entrepreneur

Sure.

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

What slide number is that?

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

It's nine.

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

Nine.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, on slide number nine, sorry Gayle, we're at – slide number nine.

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

Okay, I'd like to address a scenario, which isn't actually addressed in the examples, but I think should be easy for us to address, which is in effect non-automatic transfers of information. So, the scenario is that a coder looks in the EHR in order to determine information in order to decide how to code something and then enters the code by hand into the billing system. That represents information from an EHR that is going to be disclosed, but I think it should be excluded in the same sense that automatic transfers of information are excluded.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, no, in your example Wes, when the coder enters that information into the billing system, the billing system is still inside the compliance environment of the covered entity.

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

It is, but it's not an EHR.

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

Well we are focusing on EHRs Wes, and we're asking –

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

That's my point. That's my point.

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

(Indiscernible)

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

My point is that we're listing the scenarios that don't trigger a need to report a disclosure and a member of the workforce looking up information in the EHR and then entering it into another – a non-EHR system, is no more – does – no more triggers a disclosure than an automatic transfer of information between the two systems.

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

Got it.

Paul Egerman – Businessman/Software Entrepreneur

In other words you're saying, you want a third bullet there –

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

Automatic or manual transfers of information –

Paul Egerman – Businessman/Software Entrepreneur

Manual or semi-automatic transfers from EHR to other –

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

...electronic systems.

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

I don't think it needs another bullet, it just needs automatic or manual transfers of information. Right.

Paul Egerman – Businessman/Software Entrepreneur

Yeah. Okay. That's a great suggestion because you're right, that example – that is a good example, because – it's an important example also because in your example the billing system is a separate system –

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

– but there are some vendors who create like total complete systems where they consider the billing system part of the EHR, it's all like there.

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

But from the –

Paul Egerman – Businessman/Software Entrepreneur

And so, again, it's consistent with the idea of following the data, the data's not being in a compliance –

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

I think it is. I'd like to make – I'd also like to make a minor suggestion Paul in the prior bullet.

Paul Egerman – Businessman/Software Entrepreneur

Yeah.

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

I'd like to suggest using his or her security credentials, such as user name and password –

Paul Egerman – Businessman/Software Entrepreneur

Yes.

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

All right.

Paul Egerman – Businessman/Software Entrepreneur

So we had somebody else make a similar suggestion in an email that – that's right, there may be other tokens or other things involved.

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

Well that and there's a whole other use of the term credentials, which has to do with how physicians are accepted to practice at the hospital and so forth. I – just adding the word security credentials helps avoid that other confusion.

Paul Egerman – Businessman/Software Entrepreneur

Good point.

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

You know – this is Dixie. Since we're only talking about electronic data, I don't understand why we can't – anybody who has – on the system is an insider and anybody who the hospital has not given an account is not, for all of these systems. If the system – if the individual is known to the system, which means they have an account of some sort, if the individual is known to the system, they're an insider. If the individual is not known to the system, they aren't.

Paul Egerman – Businessman/Software Entrepreneur

Well that's right Dixie, although sometimes it's not an individual. In other words, when you – data through an HIE organization or you submit it to an insurance company, it's information simply transmitted outside of the organization to some other computer somewhere.

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

This is Judy, right now. Can I interrupt for a sec?

Paul Egerman – Businessman/Software Entrepreneur

Sure, go ahead.

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

Okay.

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

But I don't – let me finish. I don't understand why if it's software – even if it's software, it's known to the system.

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

I don't understand your misunderstanding Dixie. Are you asking a question or –

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

It would be – I'm just saying, I think it would be clearer than the compliance environment. I think that's hard to understand.

Paul Egerman – Businessman/Software Entrepreneur

So you're just considering – you want us to word compliance environment differently, you're sort of tripping over that expression.

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

Yeah, I think it would be more universally understood, yes.

Paul Egerman – Businessman/Software Entrepreneur

Okay.

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

I think we can add a lot – I mean, I don't think we need to necessarily get rid of the term, but I think having more explanation around it will help.

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

Yeah, I do, too. Yes. Yes.

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

That's helpful Dixie, thank you.

Paul Egerman – Businessman/Software Entrepreneur

So, Judy you were trying to break in here.

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

Yeah, two things. One, this is maybe already covered, but, on slide 8 where it says use the data for internal purposes, would it make sense to add, other than quality review? Because it does make sense that people would do that. Secondly, I'm thinking a bit about ACOs and the whole move to population health as we're talking about this, which means that you have a group that's not on an OHCA, not on your OHCA, but it is another group with whom you share the care of that patient. And you are going to be held responsible for the risk and outcome of that patient among everybody who is taking care of that patient in the ACO. I wonder whether we should be addressing that at all.

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

Well Judy, that – the bearing of risk is a qualification for being an OHCA. So if you're in a risk-bearing ACO and you haven't taken whatever HIPAA steps necessitate you being an OHCA that would surprise me.

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

Okay, so what you're saying is, even though they're not on the same system –

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

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation
– because they're combining the care of the patient as an ACO, that's okay.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology
If, if – right, I mean I'm – again, ACOs have different aspects to them –

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

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology
– but the ones bearing financial risk would trigger a definitional prong under HIPAA's definition of OHCA.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation
Interesting, okay.

Paul Egerman – Businessman/Software Entrepreneur

And also Judy, not – I don't – I hope we're not interrupting your train of thought, but the idea of being on multiple systems is important. This is also – this approach is also intended to address the example of what I understood to be possibly the current environment like at Intermountain Healthcare where you might have lots of different computer systems at lots of different locations doing various functions. And it's – somehow they're all Intermountain Healthcare, so that's all internal –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation
Yeah, that's internal.

Paul Egerman – Businessman/Software Entrepreneur

– moving from one thing to another, move data around is no – we're saying that's not a disclosure you want listed.

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

Now here's another variation of that. One of the worries that the folks in the OHCA's have is that they are responsible for the risk of a patient they are not treating. And so I'm assuming then that if you're in a risk-bearing situation with others, even if that patient isn't your patient, you can still look at that patient's record, because you bear risk for that patient. Is that accurate?

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

That's a different question about whether you can actually access a record and the question – the answer to that question is yes, that it's a tr – if you're treating a patient –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation
No, you're not treating them.

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

Well only a cer –

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

You're at risk for them without treating, which is really one of the worries that a number of folks in OHCA's and ACOs have, they may be responsible for a patient without ever seeing that patient.

Paul Egerman – Businessman/Software Entrepreneur

Well –

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

Interesting question Judy, but not related to the issue of which disclosures would be on a disclosure report for our recommendations.

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

Because this organization then can see my records at my other organization and I've never gone to that first organization.

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

Yeah, but Judy, it's a different question about the legal –

Paul Egerman – Businessman/Software Entrepreneur

But here's how I'd answer that – I'd answer that –

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

Well it's still a disclosure question.

Paul Egerman – Businessman/Software Entrepreneur

I'd answer it in the environment of the analogy like a staff model HMO. If they have a record on a patient, but the patient is never seen at that organization, then there's nothing to disclose, because – the data –

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

Oh no, but they're looking for the data to figure out, am I charging the right amounts? Are –

Paul Egerman – Businessman/Software Entrepreneur

But that's all internal stuff. In other words, it only is a disclosure –

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

So that's okay?

Paul Egerman – Businessman/Software Entrepreneur

– when it leaves the entity. And so, if they never treat the patient I don't understand how the data ever leaves the entity or why it would.

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

Okay, I see what you're saying – or maybe it has to for them to be able to assess what – how they're doing financially.

Paul Egerman – Businessman/Software Entrepreneur

Well, I mean –

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

John, what about you?

Paul Egerman – Businessman/Software Entrepreneur

– if they send it to some registry or something, then it is a disclosure. I mean –

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

– again, one of the things we've got to keep in mind is what we're trying to do here. The problem with the disclosure report as it was talked about in the NPRM was, you ended up with a report that's like probably 20-30 pages long, with all kinds of stuff that was just – was not useful to a patient to know about, plus to read it would be very confusing. What we want to try to come up with is a document that is much shorter, to me the ideal is like 1-page long, and says to the patient, well here's your data, here's where it is. The patient is at A, B, C medical group, but it's at this HIE, it's being sent to this insurance company, it's going to this registry and this data intermediary and you list out where it is and that's our intention. That it's a disclosure report that will be useful to people and will be useful if it has the right information on it.

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

Okay.

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

This is John Houston. I have a couple other unrelated comments to the last couple of slides if we're done with that.

Paul Egerman – Businessman/Software Entrepreneur

Okay. I think Judy said she was okay, so go ahead John.

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

There were two examples on slide 7 and 8.

Paul Egerman – Businessman/Software Entrepreneur

Okay, so let me go to slide 7.

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

Okay. It says data's moved from a provider to a HIE and then the second one is on slide 8, which describes limited data sets being created, which I think is the last bullet.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, let's do them one at a time.

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

In each case, I believe that many examples of that will be where the organization is a business associate of the covered entity –

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

Yup.

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

– and as such, they would be under the control of that covered entity. And I don't think that those would trigger a reporting as long as they are a business associate.

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

You know John, its Deven. Were you on our last call?

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

I was not, I apologize.

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

No, so when we initially had some conversations about the follow the data concept, there was some discussion about whether we would try to make a distinction between arrangements where say a business associate receives the data, but doesn't have the capability under their business associate agreement to use it for any other purpose, other than some specific purpose delineated by the covered entity. But there was concern by other Tiger Team members that in fact the mere transfer of that data to another entity where that entity could have the capacity to say, de-identify the data and use it for other purposes or it might not have as secure an environment was the better way to approach this issue. As opposed to drawing lines around business associates where there's tight control versus business associates where in fact due to inequities in bargaining power, you have a business associate with a lot of control over the data going forward. Notwithstanding how difficult it is for a computer to make that determination.

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

And I absolutely appreciate that nuance, I just think that there are – the typical business associate relationship, there is a lot of control. And I agree that certain of these accrediting organizations will try to reserve the right to do limited data sets and de-identify data and use it for all sorts of other purposes, which I don't like myself. In fact, I'm one of the primary advocates that that practice should stop. I just think somehow though, that where there is a high degree of control over those business associates, and I think it does occur with HIEs that I personally don't think that that amounts to a disclosure. And there will be certain cases where a business associate does create limited data sets on behalf of the covered entity under very strict controls, where I don't think that's triggered either. So, I don't know how we deal with that nuance and how we – that continuum, but it just seems to me there's – I can see both sides of that.

Paul Egerman – Businessman/Software Entrepreneur

And so John, if you look at – data, we are saying that if the recipient has the ability to disclose the data to other covered entities, resell or otherwise monetize the data, that that is a disclosure. And –

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

Well that is – I'm looking at the very last one.

Paul Egerman – Businessman/Software Entrepreneur

Yes, you say that may not necessarily be one.

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

So maybe –

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

Well that's right, but Paul, it gets to the heart of, I think, it may be worth just noting for the committee that there was a desire on the part of some folks to try to make a distinction between those business associate arrangements where the entity retain – while the data may actually move from the entity to the possession of the business associate, but it's under very tight controls. And that that's quite different from an arrangement where the business associate in fact controls the data and reserves certain rights to it, whether that's part of the BAA or it's just unspoken in the BAA and done as a matter of practice. But it's hard to draw that line and we certainly can acknowledge that that's a possibility, even while we think that a follow the data approach is the one that probably makes the most sense to try to pilot.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, I think –

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

Can I suggest that –

Paul Egerman – Businessman/Software Entrepreneur

– I think that's right. But in looking at this also, one – and I don't have – I think it certainly makes sense, we have to reflect what the members of the workgroup think, and so we can make that comment here. Again, it is my opinion, it still goes back to what is good disclosure for the patients. If the data is going to an HIE, I think that should be disclosed and the way it could be disclosed though, is, I mean, I suggested this before. You could have a blanket disclosure, you could say something like for the past three years we send all of our test results to ABC health information organization so other providers can have access to them. I mean, you could do a one – you could have a series of one sentence blanket disclosures. It doesn't mean that you have to – in fact, that's probably far better than simply saying, on this date we sent the LDL over and on this date we sent the hematocrit over, that's excessive amount of information that nobody's going to really – I don't know whether or not anybody really wants it. And so that's – my comment is we want to keep in mind what we're trying to do is make sure patients know where their data is.

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

Can I suggest that maybe this slide 8 there's just a couple of really minor tweaks we could do that'll clarify this?

Paul Egerman – Businessman/Software Entrepreneur

Okay.

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

After the words who will, maybe say the independent ability to –

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

Yeah, I agree.

Paul Egerman – Businessman/Software Entrepreneur

Oh, that makes sense. That's a good suggestion.

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

Good.

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

And then on the bottom one, create limited data sets of de-identify the data for independent purposes or purposes unrelated to the covered entity. That makes it clear that they're using it for their – the covered entity isn't the one that's going to be the recipient of the – data.

Paul Egerman – Businessman/Software Entrepreneur

So those are helpful comments, very helpful. Thank you.

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

Yes, good.

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

This is David. It occurs to me that what we're describing is not so much follow the data but follow the control of the data.

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

Good point.

Paul Egerman – Businessman/Software Entrepreneur

That's true David, but I think that you have – don't we have to do it that way now because it's like in one sense you can't follow the data because there's like – the data's like virtual. It could be a lot of different places and a lot of different copies, so it's really sort of like, who has some sense of control. And you can't even use the word ownership –

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

Right, right.

Paul Egerman – Businessman/Software Entrepreneur

– because that also is – doesn't quite work with data, so it is an issue of follow the control of the data.

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

And since you gave me the floor, I have one other suggestion that's just a minor point, but I think it's consistent with what we just said. Its back on slide 6, in the red where you say when a provider sends a copy of the data from an EHR outside, we don't really want to imply the limit that it's only provider initiated sends, right? It's when control of that data moves to an outside entity, right?

Paul Egerman – Businessman/Software Entrepreneur

That's right.

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

So –

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

Yeah, I think that's a great improvement.

Paul Egerman – Businessman/Software Entrepreneur

Yes.

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

Got it, thank you. That's great.

Paul Egerman – Businessman/Software Entrepreneur

That's very helpful. Excellent. So, are there any other comments about follow the control of the data?

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

Good pick-up Paul.

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

Okay, if there isn't, I mean I'm assuming silence means that people are somewhat comfortable, we may not have it perfect, but we have a good approach here. What I want to do is – the slides have been – somebody's moving my slides for me here.

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

Me, sorry.

Paul Egerman – Businessman/Software Entrepreneur

I'm going to jump to the right of an investigation. Okay, so this is slide 12.

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

Thank you.

Paul Egerman – Businessman/Software Entrepreneur

And so what we've talked about so far is the accounting of disclosures report notice, what happens when the stuff goes somehow outside. So now we're going to talk about what happens with the internal stuff for a minute. So this is the things that are inside the control of the entity, and I just want to be clear on the changes that we are making, to make sure everybody is comfortable with that. First you see on slide 12, the area in red, this was suggested by Gayle. We thought that the entity has a responsibility to do an investigation at the request of the patient or a consumer individual and then in red we said that such an investigation should enable patients to ask whether a particular individual possibly inappropriately accessed their records. So that might be, the example that maybe somebody has like an ex-husband, an ex-wife, they have somebody working at the institution and they have some reason that they're a little bit nervous about it and say, can you tell me if this person is looking at my record. So we added that in our recommendation.

And then on the next slide is how we tried to respond to Dixie's suggestion also, so that in order to improve the ability of covered entities to do this investigation, we're making a recommendation, actually to the Office of Civil Rights. So it's nice to make the recommendation to OCR that they add to implementation specifications to the audit control standard. And these are – the first one is, that – and its addressable that audit controls must record PHI access to the granularity that the individual user and the individual whose PHI is accessed is identified in the audit control. And the second is that information recorded by the audit controls are – have to be sufficient to support this sort of investigation process that we are talking about. And so just want to make sure that people understand that that's what we're doing and that everybody's comfortable with it. And so the silence –

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

Looks good.

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

(Indiscernible)

Paul Egerman – Businessman/Software Entrepreneur

– the silence either means everybody's on mute and doesn't realize it or everybody agrees. Is somebody trying to respond?

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

This is David, I was on mute and didn't realize it. I lost the slide numbers here.

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

Slide 13.

Paul Egerman – Businessman/Software Entrepreneur

I'm on slide 13.

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

I'm on 13, but which was the previous slide you showed?

Paul Egerman – Businessman/Software Entrepreneur

Slide 12.

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

Okay, that makes sense. Okay, yeah, so someone raised to me the concern, and if this is a wordsmithing, maybe that should be left to a regulatory process, but. The right of an individual investigation of any alleged inappropriate access, there was a concern from a delivery organization that any alleged is too broad and that maybe it should be appropriate or qualified or something like that. I'm not sure that's a concern at our level of detail, but it was raised to me by one of our clients, that that's an awfully broad statement.

Paul Egerman – Businessman/Software Entrepreneur

Deven, do you want to respond to that?

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

I don't understand where they wanted appropriate to be inserted.

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

I think it's the notion that there's some process or due process to determine whether the investigation is warranted.

Paul Egerman – Businessman/Software Entrepreneur

I'm wondering if you could solve this by getting rid of the why, investigation of an alleged inappropriate access?

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

Yeah, that might be sufficient softening, yeah.

Paul Egerman – Businessman/Software Entrepreneur

I mean, I guess you're looking at the situation where for some reason you have a consumer who's making a repeated request, for example, and you've already investigated. Now they're asking for the same thing again –

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

Right.

Paul Egerman – Businessman/Software Entrepreneur

You should be able to, well, I've already done that.

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

Well I don't think it would be unreasonable –

Paul Egerman – Businessman/Software Entrepreneur

Or there's some circumstance that makes you turn it down, for some reason, I don't know, maybe –

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

Yeah, there's some process that determines which ones merit full investigation and that's –

Paul Egerman – Businessman/Software Entrepreneur

Or maybe the patient's a convicted felon and you think there's – that it's really not the right thing to do under those circumstances or something.

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

I think we could just get rid of any and it should do it.

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

Did you have something else David or was that the only issue?

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

That's the only one I've got so far. I'm still rereading and rethinking. So, let somebody else talk.

Paul Egerman – Businessman/Software Entrepreneur

So did I go through this too fast, do people need a little bit more time to look at what it says here? This is important, because basically what we're saying is, we threw away that access report, but we replaced it with a somewhat strengthened concept that the organization has responsibilities to investigate the possibilities of inappropriate access. And –

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

What does –

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

So this –

Paul Egerman – Businessman/Software Entrepreneur

– to address patient concerns and we also have suggestions for increasing the audit controls.

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

So this is David and I will make a second point that I'm not as – I haven't thought as deeply about. But in slide 12 the red middle bullet, enable patients to ask whether a particular individual inappropriately accessed their records. I mean, we did back off from disclose the name of everyone who has accessed your records, but this just turns it into a probing problem rather than a direct reveal. So I wonder are we – have we just trans – have we just made the discovery of the individuals who've looked at your records a little harder, but not impossible by –

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

Well –

Paul Egerman – Businessman/Software Entrepreneur

No – again, the example is, when you have a – this was Gayle's suggestion, but you might have a reason that you're concerned about a specific individual.

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

Right.

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

Right.

Paul Egerman – Businessman/Software Entrepreneur

You have – it's just like – I don't know, you had a dispute with your neighbor and your neighbor is suing you because your tree fell on his lot. And you have – and it's really ugly and now – but your neighbor also just happens to be like a surgeon at the local hospital and you just want to make sure that he or she isn't looking at your records. So you go to the covered entity and say, my neighbor Jane Doe is a surgeon and please make sure that she's not looking at my record.

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

Yeah, as long as it's wrapped in language that prevents you from just providing a list of the hospital directory and say, I'm concerned that one of these people accessed my records, can you tell me which ones?

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

That would become the accounting of disclosures generally.

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

Right.

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

I think this is a great way to frankly cut down on effort, cut down on making a much more effective approach at people being able to understand who's looking at their record. This is what happens in our environment, so I think this is a great suggestion.

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

Yeah, this is Wes. I have a concern that I think we can address, but scenario is, it – that something is published in a – somewhere that's private information of the individual. That information clearly was gathered at the hospital, it says what procedure they had at the hospital or something else, and – but they don't have a clue as to who it was. So it seems that there are times when you should be able to ask the hospital, and maybe this is covered other areas, but it seems like you should be able to access the hospital saying, I don't know who disclosed my data, but someone did.

Paul Egerman – Businessman/Software Entrepreneur

Yes. Yeah, but that is –

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

Well right, and –

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

But can –

Paul Egerman – Businessman/Software Entrepreneur

So go ahead Deven.

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

I mean, well this was Gayle's comment, so I want to make sure that her point in raising it was covered. But I know that when I tried – when I, and I'm the one who phrased it this way. I was trying to enable the patient to prompt a question about a particular individual and to be able to have that investigated, if they wanted to. Versus saying – having it be like an access report where the patient gets a list of –

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

No, I completely agree that this is a much better way to deal with the general request of an access report for unstated purpose. Okay –

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

Yeah.

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

– I just think that we also need to be able to provide some channel – we don't want this to preclude a patient coming to say to an institution and saying, my information was disclosed, I don't know by what individual. I'm not asking for a list of all the individuals that saw my information, I'm asking you to figure out who disclosed it.

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

Can I suggest –

Paul Egerman – Businessman/Software Entrepreneur

Yeah, and that's right and I think that is intended here, maybe it's not clear. So that's what I –

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

Could I –

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

I –

Paul Egerman – Businessman/Software Entrepreneur

– read as the introductory –

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

Excuse me, this is Joy.

Paul Egerman – Businessman/Software Entrepreneur

– it says the Tiger Team reinforces the importance of the right of an individual to an investigation of inappropriate access.

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

Can I suggest –

Paul Egerman – Businessman/Software Entrepreneur

So I agree.

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

Can I suggest, this is John Houston, that we simply add, whether a particular – such investigation should enable a patient to ask whether a particular individual inappropriately accessed their records or, who accessed their records in a particular circumstance.

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

That's a good suggestion.

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

That works.

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

Yeah, I think it's pretty clear from the main bullet, but I would like to a – no, I'd like to ask what we mean by – what we expect to happen as a result of our reinforcing this importance?

Paul Egerman – Businessman/Software Entrepreneur

We –

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

I – go ahead Paul.

Paul Egerman – Businessman/Software Entrepreneur

What we expect to happen is we want to make it clear that that is a replacement of the access report. The other thing we expect to happen is what you see on slide 13, is by reinforcing the importance, we're suggesting that OCR improve the ability of covered entities to do the investigation –

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

Okay, yeah, yeah, yeah.

Paul Egerman – Businessman/Software Entrepreneur

– by making some recommendations – implementation specifications about audit control standards.

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

This is the moral equivalent of an access report.

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

So it goes together, yeah, I see. I see what you're saying, yes.

Paul Egerman – Businessman/Software Entrepreneur

In other words, they go together. In order to do what's on slide 12, we're suggesting just you take the audit – the existing implementation specification and give it a little bit more muscle.

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

This is Gayle. I'd just like to comment. I think this is a very important part of what we're doing. If you're not – if we're simply going to say, not be very specific, then you're missing the point. You need to empower patients to receive this information and I happen to believe it's extremely important.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, I agree Gayle. Because we also have to be responsive to the patient advocates that we heard in the hearing who expressed some concerns that patients had, so we're saying, well, here's part of how we'll respond to that. Once – since we got rid of this confusing access report, but on the other hand, we're clarifying and a little – we're strengthening the audit – the implementation specifications, things we're recommending –

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

Hey Paul, you're hard to hear.

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

Yeah, you are hard to hear, you're drifting away Paul.

Paul Egerman – Businessman/Software Entrepreneur

Okay, so again what I'm saying is, we are responding to the patients by clarifying what is really an existing right for investigation, but we're suggesting strengthening the audit specification for OCR, because we have to – we do need to respond to the legitimate issues that were described at that hearing.

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

So speaking of the issues described at the hearing, we are making a – in these addressable implementation specifications, an addressable, but still security rule recommendation that'll apply to electronic data. Are we sort of stepping into a technical capability issue, the same one that triggered the access report controls in terms of sort of what audit trails typically track and what kind of retrofitting might be required to do this?

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

We had that conversation Deven, about how even today – in fact, this was addressed even in the hearing. Even today hospitals have the capability, if they have a celebrity of some sort, they already keep the audit record to that level of granularity.

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

But is it –

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

They've always had that capability, they just don't review it normally. I think –

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

– or necessarily deploy it across all patients.

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

I – my experience is that they keep the same level of granularity on the VIP patients and the well-known patients as they do on every patient.

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

Yes.

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

Okay.

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

I agree with that. It's –

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

Been a gut-check here.

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

It's just the level of auditing that occurs on those records that may differ.

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

Right. Yes.

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

Somebody's –

Paul Egerman – Businessman/Software Entrepreneur

That's right, and John, when you say the level of auditing is – to clarify, it's like the level of attention that is paid to them.

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

Exactly.

Paul Egerman – Businessman/Software Entrepreneur

– you could look at these things like once or twice a day to see what's going on –

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

Yeah, the review of what's recorded versus what's recorded.

Paul Egerman – Businessman/Software Entrepreneur

But it's actually hard to record something different for those patients than the other patients.

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

Right. I mean we just – we actively –

Paul Egerman – Businessman/Software Entrepreneur

– have the same controls for everybody.

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

We just actively alert when somebody accesses a record of a VIP. So we actually give a notification when somebody looks at something – somebody's record who's a VIP, that's what we typically do. But they will get the same alert then after that point.

Paul Egerman – Businessman/Software Entrepreneur

Okay.

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

So – this is David. Back to slide 13, addressable point one, audit controls must record PHI access activities to the granularity of the individual user. Now so this is – we're talking now about internal audit, right?

Paul Egerman – Businessman/Software Entrepreneur

Exactly.

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

And what are we – are we implying by user that we are excluding automated access by decision support systems or pumps and vital sign monitoring systems and things like that? Are we –

Paul Egerman – Businessman/Software Entrepreneur

Yeah, apparently because – I think so because I don't think that that really is a part of an investigation or –

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

Yeah, so that's my – when we say user, we mean human.

Paul Egerman – Businessman/Software Entrepreneur

Yeah. That's a good point.

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

Yeah, it is a good point.

Paul Egerman – Businessman/Software Entrepreneur

And it think you do mean an individual, parentheses –

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

Human.

Paul Egerman – Businessman/Software Entrepreneur

– individual user parentheses person.

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

Yeah person, yeah.

Paul Egerman – Businessman/Software Entrepreneur

To make it clear that a corporation is not a person, but an individual user, human being, that – because the – because that's just an important point, I agree.

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

It would be if there is a human. I mean typically an audit trail records subjects accesses to objects, right? And so – so if it is – if the subject is a human, it'll record it as a human, but it would also record if a process accesses it, too.

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

But some of those might not –

Paul Egerman – Businessman/Software Entrepreneur

– Dixie, but different systems might record that differently.

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

Right, right, right.

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

Okay.

Paul Egerman – Businessman/Software Entrepreneur

And we're not trying to interfere with how they do that.

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

Right, we aren't trying to say you have to filter out all the non-human accesses because typically that – they'll record those as well.

Paul Egerman – Businessman/Software Entrepreneur

That's right, so we're just saying that you have to at least record the human ones though.

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

Yes.

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

I don't think it's universally agreed that they record the non-human ones because you see the – places the number of HL7 transactions by example and things like that that occur, they're massive, an organization couldn't, I think.

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

Yeah, and that's what I was trying to get at, there's an awful lot of automated system movement of data that's not of interest here.

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

Well we're – I think we're talking about the level in the stack, the OSI stack you're talking about. At the operating system level, yeah, that audit trail at the operating system level will record when a process accesses an application, right? But the recording of individual user's access to individual records is at the application level.

Paul Egerman – Businessman/Software Entrepreneur

Well, and this is Paul –

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

Right, and some applications –

Paul Egerman – Businessman/Software Entrepreneur

– whatever level it is, that's not – all we're saying here is you have to at least –

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

– have an audit control, somehow that you know is addressable, somehow – you have to somehow have some audit control that records a human being –

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

– accessing a specific person's PHI.

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

Yeah, we're talking –

Paul Egerman – Businessman/Software Entrepreneur

That's the level of granularity that is needed, and I think that's mostly what you have already, in fact, I think it's like almost everywhere has that already, but we're making it clear that that's what's needed.

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

Yup.

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

Okay. I have a question on a discussion we just had on slide 12, just to be clear, but I don't want to do that until we're leaving slide 13.

Paul Egerman – Businessman/Software Entrepreneur

Okay. So are we ready to leave slide 13?

W

Um hmm.

Paul Egerman – Businessman/Software Entrepreneur

I think people are disappointed, they wanted to talk about the operating system level a little bit more, but let's go ahead.

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

(Indiscernible)

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

Thanks Paul. So here there was a discussion about adding some language that – and I wrote down in my notes, so that an investigation should enable patients to ask whether a particular individual inappropriately accessed their records, or who accessed their records in a particular circumstance.

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

Right.

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

So is this not a mini-access report?

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

This is John Houston.

Paul Egerman – Businessman/Software Entrepreneur

It might be – instead of saying who accesses, is what happened to the records under a particular circumstance. They may not know, if something's published in the newspaper, part of the answer could be, well, we don't really know. But, maybe they do know because maybe what was published is very – there's some circumstance about it that might – you might be able to understand about it.

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

Okay.

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

This is John Houston. I think the best example is, somebody says, you know I came into the emergency department on such and such a date and I'm afraid that somebody may have viewed my record based upon that emergency department encounter or I'm concerned – that it – there'll be specific circumstances somebody will bring to your attention. And it may not be a person, but they'll have some understanding of when something occurred or the circumstances around which something occurred, but they're not sure who.

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

Got it. Okay, that makes sense. Thank you for the clarification.

Paul Egerman – Businessman/Software Entrepreneur

Okay, do we have any oth – again, as Gayle said, this is very important. Do we have any other comments about what we're talking about here for the investigation? Okay, well once again, I'll assume that silence means either everyone has their phones still on mute or we have agreement. And so I think we just have completed, actually a very interesting and challenging topic and I feel really good that we've got a good set of recommendations to come out of it. Do we want to – do you have anything else you want to say Deven? Do we want to open ourselves for public comment?

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

We do need to open for public comment. I guess the one other thing I want to do, Paul, since this is your last Tiger Team call is to thank you for all of the hard work that you have done over the many years we've been together and your leadership of this group. And you're helpful guidance in getting so many – helping us get so many recommendations before the Policy Committee it's just – it's been awesome to have you.

Paul Egerman – Businessman/Software Entrepreneur

Well, that's very kind of you to say Deven, but I would just tell you that I very much enjoyed working with this great group of people, and you in particular. But the entire – all the members of the Tiger Team who are spending so much time and energy and intellectual concentration on these issues to try to get them right. So, it's a wonderful thing that is going on here.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

Paul, this is Joy and on behalf of ONC, I'd also like to extend you our great gratitude for your leadership over the last many years. You've been on this team for quite a while now and we've really seen it change to a really very operational, efficient workgroup that has produced a ton of recommendations that have been acted on by HHS, which I think is a tribute to the value that you and this whole Tiger Team bring to this process. So, thank you very much.

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

Paul, this is Judy and you can't leave.

Paul Egerman – Businessman/Software Entrepreneur

Say again Judy?

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

You can't leave.

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

And this is Gayle – I'm in on that, too.

Paul Egerman – Businessman/Software Entrepreneur

Well, ONC has asked me to do something else.

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

No, you can't, you can't leave us.

Paul Egerman – Businessman/Software Entrepreneur

And so I will be responding to what ONC is asking me to do, but as I say, it's been a pleasure.

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

Paul, run fast, run fast.

Paul Egerman – Businessman/Software Entrepreneur

Pardon me?

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

Run fast.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

I take it that was John Houston.

M

In fact it is.

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

That's me. He's going to get caught in here if he doesn't.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

All right.

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

– my job Paul, we're going to miss you. This is terrible.

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

Yeah.

Paul Egerman – Businessman/Software Entrepreneur

Why don't we see what we have for public comments?

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

Yeah, on that note, maybe it's – let the public praise you, too, Paul. Altarum, ONC, want to go ahead and open our lines.

Public Comment

Christianne Williams – Business Analyst – Office of the National Coordinator

Yes, operator, can you please open the lines please?

Ashley Griffin – Management Assistant – 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 public comments at this time.

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

All right. For those of you on the Policy Committee, I'll see you on Wednesday and otherwise, I'll be with the Tiger Team on our next call. Hopefully we will be successful in presenting these recommendations to the Policy Committee on Wednesday. Cross your fingers.

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

Thank you.

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

Thanks.

Public Comment Received During the Meeting

1. While an ACO may well be an OHCA, I do not believe that being an ACO necessarily makes the organization an OHCA.

2. Header for Slides 9, 10, 11 should stipulate which "report" are you discussing? Report: Accounting of Disclosures, or an Access Report?