

**Privacy and Security Tiger Team**  
**Draft Transcript**  
**April 6, 2011**

**Presentation**

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Good afternoon, everybody, and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Call, so there will be opportunity at the end of the call for the public to make comment, and just a reminder, please, to workgroup members to identify yourselves.

Quick roll call. Deven McGraw?

**Deven McGraw – Center for Democracy & Technology – Director**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Paul Eggerman?

**Paul Eggerman – Software Entrepreneur**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Latanya Sweeney? Gayle Harrell? Carol Diamond? Judy Faulkner? I heard her earlier. John Travis from Cerner.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Neil Calman? David Lansky? Dixie Baker?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Micky Tripathi? Rachel Block? Alice Brown from National Partnership?

**Alice Brown – National Partnership for Women & Families – Director HITP**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

John Houston?

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Wes Rishel? Leslie Francis?

**Leslie Francis – NCVHS – Co-Chair**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Lisa Tutterow?

**Lisa Tutterow – Office of the National Coordinator – popHealth Principal**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Adam Greene? Joy Pritts? Did I leave anyone off?

**Judy Faulkner – Epic Systems – Founder**

This is Judy Faulkner.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Deven and Paul, over to you.

**Deven McGraw – Center for Democracy & Technology – Director**

Thank you very much. Thank you tiger team members for joining. Thank you for folks who are serving instead of tiger team members who couldn't make the call today, and thanks as always to the members of the public who listen in on our calls and provide us with feedback. It's very helpful.

This is the last call before the April 13<sup>th</sup> Policy Committee meeting. We have a two-hour call today, and I think a manageable set of issues to tackle in the timeframe if we are efficient in our discussions, which I think we can be. We're basically following up on some conversations that have been ongoing for several of our past meetings, but most importantly, on our last meeting we got to some resolution on a number of recommendations that are specifically related to EHR functionalities that might need to be considered for some additional stage two certification recommendations. Essentially what I did, was to take the draft recommendations that had been circulated to you in advance of our prior meeting and to mark them up using track changes with some of the additional points that were made during our last call, which was last Friday. That is the document that you received from ONC, and that you can also identify if you're looking on the Web screen, it's on the download list. It's the first document. It says, "Identity auth, digital cert, and patient matching." Essentially, that is the collection of all of the recommendations that we think we have closure on. Based on the consensus reached on previous calls, there is some additional explanatory wording that is based on discussions that we had during our last call.

Given the time constraints that we're facing and the need to make some progress on some additional recommendations before we can declare ourselves to be finished and ready for next Wednesday's Policy Committee meeting, we're not going to spend time wordsmithing those on this call. So that I'd ask you, in the offline time period, to take a look at that document, if you haven't done so already, and make sure you give me feedback on any of the additional language. Again, it's all tracked so you can see it, and let me know if you have any significant concerns or suggestions about it.

Then given that, our plan is to really spend this meeting focusing on the recommendations that we really didn't get to consensus on in the last meeting. That is the issue of whether we want to add something more to the requirement to do a security risk assessment that addresses some of the addressable implementation specifications in the security rule and then some security policies with respect to patient portals, which are contemplated for stage two of meaningful use.

So, I want to stop there and first ask Paul if he has anything to add.

**Paul Egerman – Software Entrepreneur**

I think that's a good summary. I love the title of the document, which is identity auth, digital cert, patient matching recs because it's a combination of our previous work and so I guess we combined it on the title also. Good summary, Deven.

**Deven McGraw – Center for Democracy & Technology – Director**

Does anybody have any questions or concerns about how we intend to move forward? All right, terrific. Well, then we'll go to the first slide in our deck here if Altarum can help us out. Then, just to—Okay, maybe the next one, the title slide. In our last call, we talked about how in stage one eligible providers and eligible hospitals need to conduct or review a security risks analysis in accordance with the security rule, implementing updates as necessary and correcting identified deficiencies. We had discussed that we wanted to include this in stage two of meaningful use, so I noted on the slide here that we consider this to be completed. But the discussion that we begin on our last call, but didn't really quite have time to finish, is whether we want to really do more of that.

We spent some time talking about how maybe we might want to add an additional requirement that shines a spotlight on the problem of the lack of encryption for data at rest, that has resulted in a number of instances of breach—of more than 500 records that have been reported to HHS since the breach notification requirement went into place. Then we have another option on the table for you to discuss, which is essentially not to just spotlight this one addressable implementation specification of the security rule, which encryption of data is one. It's an implementation specification that's addressable. But, in fact, to sort of expand that to really talk about all of the addressable—and I frame this as addressable provisions, but really—thank you Dixie for your helpful input here, but—we're really talking about the addressable implementation specifications that are part of the HIPPA Security Rule.

So, we have those two options on the table although there might actually be a variation that we also might want to talk about, which is not necessarily to spotlight all of the addressable implementation specifications, but instead to spotlight all of those that are tied to certified EHR functionality. So, I'll mention that, that we didn't think about that in time to make it into the slides but you please keep that in your frame of mind as we begin to discuss these options.

I just wanted to note that before we begin the discussion of the two options, Adam Greene—Adam did you join the call in the interim after we did roll call? Okay. Adam Greene, who is typically on our calls, and has been on the previous ones and is well aware that this is on our slides today and in our documents. In a presentation that he made, the HIMMS Annual Meeting, which just took place a month ago, he noted that an entity (either an eligible professional or hospital) that manages a certified EHR system that has built-in technical safeguards for confidentiality, availability or integrity of electronic protective health information will be expected under the HIPPA Security Rule to have those system safeguards in operation. So, this is an indication of his interpretation of how someone with a certified EHR is charged with implementing an addressable implementation specification when you've got the technology right at your fingertips. So, I wanted folks to have that information in their minds as well, because there's many policy levers that HHS has potentially with respect to privacy and security policy, and certainly enforcement of the HIPPA Security Rule is one. Then of course, the meaningful use provisions and the certification provisions are yet another.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Tell me if I'm out of order and if you want to discuss it later, but that statement by itself leads to a number of concerns. For example, if an EHR offers multiple ways of achieving a security goal, is the hospital expected to use all of them? That would be an easy question to answer if each capability of the system was solely identified with an individual security goal but it's not usually the case. I don't know whether that's in scope for us to discuss or not.

**Deven McGraw – Center for Democracy & Technology – Director**

I don't think it's in scope for us to discuss only because— The reason why I offered it here, Wes, was to give the tiger team members and the members of the public listening on the call a sense of where staff at the Office of Civil Rights are. With respect to how someone who has a certified EHR, that has certain security functionalities built into it, what does that mean when they approach addressable implementation specifications under the rule, which are not required—doesn't say, per se, thou shalt do x, y and z. I recognize that—expect that the language here suggests that the expectation is that you would have all of them in operation might actually not be either possible or advisable from a security standpoint, but for us to get into the minutia of whether this is good policy or not good policy, I think, is out of scope.

The reason for offering it is to just get a sense of how—number one, something that's addressable under the security rule doesn't mean that it's optional, number two. I think it's an indication that, to the extent that what the standard is under the rule, with respect to implementation specifications that are addressable, is you're supposed to implement them if it's reasonable and appropriate to do so. If it's not then you're supposed to find an equivalent alternative that is reasonable and appropriate to do so. That's the standard. I think what they were getting at here is, if you've got the technical functionality in your EHR and you choose not to turn them on, as is the case, you're going to have to have some decent justification if you're audited for why you chose not to do so.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

So, perfect, not only have you indicated why it's not appropriate for today, but you've fully disclosed of the issue as well.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, good.

**Judy Faulkner – Epic Systems – Founder**

Deven, I've got a question for you. From a development point of view, you can develop systems that when you put them onto a report you can encrypt them as they go onto laptop or whatever. I don't have one of our developers with me, and it's been too long since I was a developer, but I think that there are often lots of ways people can get into systems and get around what you do. For example, perhaps you can shift the data to a system that's going to do report generation analysis on it and that isn't encrypted because the EHR vendor doesn't control that. Is it planned that, there is no way around it, that that's understood, that there will be some places that will have leaks in them?

**Paul Egerman – Software Entrepreneur**

Let me respond to that. I think it is understood, Judy, is the way we are talking about shining a spotlight on encryption data at rest is this, an attestation by the provider as part of meaningful use.

**Deven McGraw – Center for Democracy & Technology – Director**

I'm going to move to that, Paul, just so we can get on the slide.

**Paul Egerman – Software Entrepreneur**

So, it's not the certification criteria, the issue there is to say—because you're exactly right. There's a lot of issues where the vendor just doesn't have any control. Plus, on top of that, it's a very hard thing to think how you do some certification criteria that you would test any software about it, because how do you really know? So the idea is just to put the responsibility on the user, on the provider, which is I think where it belongs.

**Deven McGraw – Center for Democracy & Technology – Director**

Just to add—so I went ahead and moved us forward in the slides here. So, we had a little bit of a discussion that John Houston prompted as well on our last call about what that unintended consequences of an out and out requirement to encrypt data at rest, and so we're not proposing that here. We're actually not proposing really to change the notion that encryption of data at rest is in fact an addressable implementation specification. Instead, what we're proposing here, is using the meaningful use criteria—to borrow the term that we used last time—to really shine a spotlight on this functionality of encryption at rest that already has to exist in certified EHR. It's part of the stage one criteria and just ask that as part of meaningful use, that providers and hospitals attest that they have in fact addressed how they're going to implement this particular security functionality. Both with respect to data in a data processing facility, for example, as well as data that's mobile such as on laptops or mobile devices.

Again, we're not suggesting that documentation be presented but an attestation that this has been done. Then, of course, they should document it because if in fact there is a question on the part of the regulators as to whether this got done, they will have to demonstrate that. So, it's a shine the spotlight approach. It is offered as an option, in part because of the—well really because of the problems that we have had even in an era post HITECH, where there is a strong incentive to encrypt data because if you

do so, you don't have to notify individuals if you have a breach of information under the HITECH Act. But nevertheless, encryption isn't happening in the healthcare sector, or it appears not to be happening at a sufficiently alarming rate that we have what we, not so jokingly refer to on these calls, as the wall of shame of entities experiencing large data breaches and most of them due to theft or loss actually. Let me go back to Paul's comment. You've lost the data, either because it's been stolen or because you've lost it.

**Paul Egerman – Software Entrepreneur**

To be specific, you've lost the media. You can lose the data without losing the media but we don't like to mention that. It's lost media.

**Deven McGraw – Center for Democracy & Technology – Director**

Thank you, Paul. So essentially, we have this as an option. Then the other option that we have on the table—just to sort of lay them out and so we can kind of discuss them as a whole—is essentially the same shine the spotlight approach. But instead of saying we're only going to do it for one particular functionality in certified EHRs, let's look at all of the addressable implementation specifications. We either cast that net really broad as is worded on the slide, and say, "Oh, it's all of the addressable implementation specifications and the security rule", or we target those addressable implementation specifications that are tied to or supported by actual functionalities that are in certified EHRs. Encryption of data at rest and in motion would be two examples of where that would apply.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Deven, I understand the encryption arguments that are being made today. My concern is that there are so many ways the data is at rest, and some data at rest has a much higher inherent risk than others at rest. I agree that in many contexts, it would be appropriate to encrypt data at rest, and I think, as I said that in a prior meeting, the mass general settlement agreement that occurred demonstrates the fact that they like to see encryption on things like USB drives and the like. However, I don't think that at rest in a data centered environment, is equivalent to, or the risks are equivalent to, or even the protection is equivalent to encryption like on a USB drive or a laptop or something like that. I think we need to be very thoughtful about when we say that that's appropriate and not.

**Deven McGraw – Center for Democracy & Technology – Director**

I'm not disagreeing with you, John, and so we try to actually very carefully word this and maybe we didn't get quite there. We're actually not setting a requirement that's beyond already what a provider would have to do under the security rule, which is to address the implementation specification of encryption, which means you deploy it when it's reasonable and appropriate to do so and you find equivalence when it's not. We're not trying to change that at all. In fact, all we're trying to do here is say, "Let's use the meaningful use program to shine a spotlight on that very same requirement."

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Okay, because ... look at the meaningful use stage one stuff, to me it really does, at least to me, speaks to the high risk areas and the need for encryption in those areas. So that was my point.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

I've been trying to figure out how to say a couple of things, and I'm reflecting on our own certification experience on these points. One is kind of a statement of, I think you really need to know what you're per chance getting through certification in stage one. Vendors really only have to test one example. They quite honestly get the ticket and most of them gravitate towards encryption of data in transit. That's explicitly tested and ONC-ATCBs will allow the vendor latitude to use that for general encryption as well, so I'm not sure encryption's being tested quite as thoroughly as you might think. So that might be something to take off and chew on, that you really are compelled to test different examples so that you really do cover data at rest and data in transit in certification effort.

The other being that, and kind of it goes with what John was saying on this slide, I've always felt something that was left unaddressed in the technical security guidance that the Office of Civil Rights provided for the breach notification rules was enterprise storage, storage area networks, large backend

storage systems. It was very, very focused on mobile computing, storage on mobile devices, etc. So I think you may want to consider if those are two specific points to really call out, what the intent is relative to certification criteria and meaningful use. Are we really interested mainly in ensuring data at rest encryption for where there's real vulnerability and encryption is the primary means of securing the data versus a storage system that might sit behind a firewall, have leased access privileges, have a lot of physical security for the data center, etc. So, there's not much distinction made there, and I think there's an intent to ensure data at rest encryption is really tested. There needs to probably be more explicit focus on that in certification being required and not something that may or may not really be tested.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes. Although I think we actually, I need to dig out the previous document—so, John, you were not on one of our previous calls.

**Paul Egerman- Software Entrepreneur**

Deven, let me try to respond. Let me be clear, what we're saying in 2A, is not related to certification. This is not about certification.

**Deven McGraw – Center for Democracy & Technology – Director**

Well, no, that's right. That's right.

**Paul Egerman – Software Entrepreneur**

It's very hard to test whether or not ... is really at rest in certification. This is entirely related to meaningful use in which the user, either the eligible provider or a hospital has to attest, and all we're asking them to attest to is just that they're following the existing regulations about this topic. The regulations are that you either have to encrypt it at rest or you have to explain why you don't do that.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Okay but then maybe I'm—

**Paul Egerman – Software Entrepreneur**

That's just what the regulations are and so people just have to attest that they're aware of it and they've done it.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Maybe, my apologies for a bit reacting into slide five then, is that it says, what you're saying is, address how you are implementing the certified EHR encryption functionalities. That's a different statement, in my mind than what you just said, and I think it's an important distinction.

**Paul Egerman – Software Entrepreneur**

Yes ... don't really want to have the phrase certified EHR encryption functionalities. You're right about that.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Yes, and that's what I was—

**Paul Egerman – Software Entrepreneur**

—because ... that part because the—so, that's where the confusion is because it's possible the way this gets implemented, for example, is some vendors might implement it with like a hardware encryption capability or something. So it's not really this certified EHR encryption functionality, you've got some other functionality that you've used, which is fine. What the goal here is, if we go back to basics, what we're trying to do is say we've got this thing called the wall of shame. It seems like it's a growing number of ... going on about people who lose a laptop, who lose ... 2,000 patients, 600,000 patients are involved. It's headline news and that reduces—it's bad for all of us when that happens because it reduces public confidence, and so what we're trying to do is remind everybody this is what they're supposed to do. They're supposed to keep track of their media. So it's not creating any new law. It's not creating any new certification requirement at all for the vendors. It's entirely just another place where the healthcare

provider has got to sign, and hopefully before they sign, they think through whether or not they've got it right.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Well, let's be careful too that we also make appropriate recommendations. I'll give you the example as you just said, do hardware encryption. Hardware encryption does nothing to protect the databases once the application starts to access them. So if you're just saying hardware encryption's my end all, be all that will prevent data that's moving outside of the data center from being taken or stolen. But it doesn't prevent things like data once the data comes off the storage device and is being accessed by the application, from being protected because a hacker could get into that data as though it was not encrypted at that level. So, we have to be careful about—

**Paul Egerman – Software Entrepreneur**

We're only worried about right here is the data at rest, and we're only worried about it because we're worried about the lost media or the missing ....

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Fair enough, Fair enough. Okay.

**Paul Egerman – Software Entrepreneur**

So it's not a discussion really of encryption. This other way to think about it is there's a problem with lost, stolen, missing media. What we'd like to do is shine a spotlight on that, and see if by doing that we can mitigate that problem with it.

**M**

Fair enough.

**Deven McGraw – Center for Democracy & Technology – Director**

Judy first, then Dixie.

**Judy Faulkner – Epic Systems – Founder**

A couple things on that. I know you it doesn't mean the transfer of the data, it means at rest, Paul, but it can be at rest when it's transferred by a programmer who can get in and get in around whatever the mechanisms are that EHR has for encrypting the data. So the trick isn't the device necessarily, a USB drive or a laptop. The trick is how does the person access that data, bring it over, and does he or she bring it over in such a way that it's protected. There's too many ways around it, and so I don't know how we address that if the organization has to make sure that if it is a laptop or a USB device that it's encrypted once it's on it.

**Deven McGraw – Center for Democracy & Technology – Director**

All right, I don't want to hone in on Dixie's comment, and maybe I'm not as familiar with the scenario that you're talking about, Judy, but I don't think we're trying to solve for every possible permutation of data access that might be unauthorized. I think we're instead just again using an existing addressable implementation specification in the HIPPA Security Rule to shine a spotlight on it because we do have a problem of media loss, that's showing up in the form of these breaches that is damaging public trust. It's not a fix that will work 100% of the time, but it's better than what's being done out there now, from as far as I can tell.

**Judy Faulkner – Epic Systems – Founder**

I think what the problem I'm seeing, Deven, is that the words in option 2A and what you say don't seem to be the same.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, well I'm fully amenable to wordsmithing this to the point where it meets the consensus that we appear to be closing in on, if I'm reading this right. Let me let Dixie say what she wants to say, and then we should work on seeing how we can get this right.

**Judy Faulkner – Epic Systems – Founder**

Yes, because it seems much stronger in 2A, what you're saying.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, that's fair. Dixie?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I think Judy's problem is with that phrase "this includes" right there that we can wordsmith, but I just wanted to say I really am strongly for including this as a stage two measure, and in particular because it addresses a very well-documented problem that we have with disclosures through media that are lost, stolen, or otherwise mobile. My comment has to do with the last part of it. I make this comment because I want to elevate the probability that this is actually going to become a stage two measure as much as we probably can. So I'm thinking that CMS may be averse to the last part of the part that says, "may be required to produce documentation if audited," because that auditing really is an OCR function not a CMS function. So I'd like to recommend that we just put "providers and hospitals must attest that they have done this as part of the risk assessment" and stop it there.

**Judy Faulkner – Epic Systems – Founder**

So, Dixie is saying it's a stage two criteria, and Deven is saying it's a shine the spotlight. Can you explain if the two are the same or different?

**Deven McGraw – Center for Democracy & Technology – Director**

Yes. They are the same. We're using the stage two meaningful use requirements to shine a spotlight on encryption of data at rest.

**Judy Faulkner – Epic Systems – Founder**

Yes. The thing I'm trying to add to it is, although I agree with the aspirations that you both have, we have to find out what's doable so we don't put things on there or at least state them in a way that can't be done because then that doesn't do anything for trust.

**Paul Egerman – Software Entrepreneur**

I agree, Judy, although the concept of what we're trying to say here with option 2A is that we're not asking for anything more than what in theory is supposed to already be happening.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes.

**Judy Faulkner – Epic Systems – Founder**

I realize that.

**Paul Egerman – Software Entrepreneur**

Yes, so I know, in some sense, in theory, if any hospital were to send in a note that says, "This can't be done. I can't do it," in theory, OCR should immediately audit that institution. They're supposed to be doing it already. What is in 2A is what people are supposed to be doing. It's like eating your vegetables or something. This is what's supposed to be going on, and we're not telling them that they have to do anything more than what they're currently required by law, in terms of vegetables, but this is one of the things they're supposed to be doing and they're not.

**Deven McGraw – Center for Democracy & Technology – Director**

Right, that's right. So I wonder if instead, the right way to frame this is to recite what is the law in terms of addressable implementation specifications and say that with respect to encryption of data at rest—and maybe we want to limit it to mobile devices. Or may we just want to say, "with respect to encryption of data at rest, as part of meaningful use stage two, providers and hospitals must attest that they have done this as part of their risk assessment."

**Paul Egerman – Software Entrepreneur**

Right, we probably should put in because there's so many violations, that is why we're asking for this.

**Deven McGraw – Center for Democracy & Technology – Director**

Why we're asking for this, right.

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

You will drop the phrase "certified EHR encryption functionality"?

**Paul Egerman – Software Entrepreneur**

Yes. I think that makes sense. I understand now why it is, I kept saying it's not certified and you kept saying it was. It's because it says it right there. Yes, ... confusing ....

**John Travis – Cerner – Senior Director and Solution Strategist, Regulatory Compliance**

Yes. That was my reaction because then you get into are you really getting what you think you're getting and you may or may not be.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay. All right, well we can fix that and, Dixie, I personally am fine with the suggestion that you had about requiring the attestation and ending the sentence there. Is there anybody who objects to that? Typical lawyer, I'm over thinking things. All right, great, thank you.

**M**

Wait, I'm sorry. Exactly where does this stop at?

**Deven McGraw – Center for Democracy & Technology – Director**

It stops after risk assessment. So, it says, "providers and hospitals must attest that they have done this as part of their risk assessment, the one that's already required for meaningful use."

**M**

Okay.

**Deven McGraw – Center for Democracy & Technology – Director**

Again, this one was one that took some time to resolve. I'll send around language by e-mail that isn't buried in a document so you can see it really easily.

**Paul Egerman – Software Entrepreneur**

Unless we go with option 2B, then we don't need 2A.

**Deven McGraw – Center for Democracy & Technology – Director**

Well, that's true. That's right. Essentially 2B is really about well why just cherry pick data at rest, security for data at rest. Why not look at all of the implementation specifications that are addressable under the rule and ask for providers and hospitals to attest that they've addressed these as part of their risk assessment as well? Since encryption is an addressable implementation specification, it would be part of this but rather than shining the spotlight on one problem that has proven to be difficult to resolve, option 2B plays no favorites and says they should comply with the law on addressable implementation specifications for all of them.

My personal thought is that—and I noted this in the documentation—this is very similar to the recommendation that the Privacy and Security Working Group of the Policy Committee, which there's a number of crossover members with this tiger team. But that's the workgroup that was in place at the time of the finalization of the stage one meaningful use rule. This is the same recommendation, essentially, that we put forward in stage one. We did limit it to those addressable implementation specifications that were supported by functionalities in certified EHRs. But nevertheless, it still was along the same lines. You're already required by law to address these. We want you to do it as part of meaningful use as well and attest that you've done so, and CMS did not accept that.

The Policy Committee accepted that recommendation but CMS did not. So, as Joy has said to us, it doesn't preclude us from offering it again, but I do think personally one of the strengths of option 2A is that it targets a persistent problem versus looking at the entire universe. But I'm amenable, quite frankly, to doing either one because I like the idea personally of doing something more in stage two than just requiring a risk assessment.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I have a question. For stage one, the requirement was that they do a risk assessment.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Does that requirement automatically move forward?

**Deven McGraw – Center for Democracy & Technology – Director**

No. This is why we already stated that it should.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay, so that's already on the— Okay got it.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes. So is there anybody who prefers not to cherry pick encryption at rest in 2A and to instead do the broader universe of addressable implementation specifications?

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Maybe a way to sort of split the middle on this is making the broader recommendation but then calling out specific ones that we are particularly interested in or think are particularly of value or note.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

That's exactly what our workgroup did, but we went through and looked at, looking at this addressable implementation spec, would the situation and the risk, would the risk change when you implemented an EHR? Those are the ones that we specifically said—

**Deven McGraw – Center for Democracy & Technology – Director**

Right, I think though that in that case—again, given that we put a fairly simple articulation of requiring providers to address implementation specifications under the rule in stage one and got it batted back down. So I would much prefer the idea of saying to CMS, we think you should reconsider your previous thinking on this for the case of, say for example, encryption of data at rest, which we know we've got a persistent problem with. I'm just concerned that a longer list, number one, dilutes the spotlight on this encryption issue, and number two, risks the same sort of global response from CMS. I'm not sure, quite frankly, that we've even had the time as a tiger team to go through what we would think would be particular policy issues on the security end that we would need to address.

So, Dixie mentions they've certainly done so on the standard side of the equation, but we have not. We would have to justify each and every one of those to the Policy Committee. I just fear we don't have the time. I'm not adverse to the idea of thinking of that more carefully about what other security policy issues need a similar spotlight. Because, again, for each and every one of them, I think we will have a Policy Committee discussion that we would need to justify them.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

I think there's a whole variety of other ones that are being under addressed, in my opinion. It requires a thoughtful discussion on each one, and I understand we don't have a lot of time.

**Paul Egerman – Software Entrepreneur**

The reason that we wanted to shine a spotlight on the one we wanted to shine a spotlight on is because of the impact it's having in terms of the news media and the lost media. It's also an impact on the patient. You get one of these letters in the mail. It's devastating. Your data is lost or your credit card information is lost. You say, "Oh my God, what does that mean?" It's very disruptive. So my view is—I guess I agree with Deven, it's sort of like less is more. We shine a spotlight on one thing and we get that one thing through, I think we've done something important. If we try to do a lot of things, I fear that what's going to happen is we'll end up doing none of them or we won't necessarily get anything a lot better.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I agree with that Paul, and I would also add that this 2B is really already required.

**Deven McGraw – Center for Democracy & Technology – Director**

They both are really.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes, but 2A addresses a very well-documented issue, and I do think it needs a spotlight shined on it. I think CMS and OCR, for sure, would have a problem with this 2B because that's exactly what's already required, so I would go with 2A.

**Deven McGraw – Center for Democracy & Technology – Director**

I heard a voice.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

You don't want to hear my voice, Deven.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

The voice thing, go with it as proposed.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

I'm just looking through the addressable requirements again just ... good example of something else we want to include. It's probably going to take me a few minutes to find the one that I'm thinking of—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Subject to John finding a killer clause here, I'll go with what Dixie said.

**Deven McGraw – Center for Democracy & Technology – Director**

Anybody else want to weigh in? All right, well let's move on. John, you can continue to look for the one you're trying to find and in the meantime, we'll move on to talk a little bit about patient portals.

Again, we've got some proposals on the table from the Meaningful Use Group to potentially require a patient portal for stage two of meaningful use. We just actually had a Meaningful Use Workgroup meeting yesterday. It appears to be squarely on the table for the inpatient hospital systems. In terms of the eligible professionals—the physicians and other professionals are eligible for the meaningful use programs—it's not a per se portal requirement, but there are meaningful use requirements being proposed that would provide patients with electronic access to their data for which a portal would be potentially one option for allowing that to happen.

So we have already put forth some recommendations on patient identity and authentication with respect to portals, and those are in the creatively named document, identity auth, digital cert, and patient matching, that we had reached some consensus on. But there are a few others that are related to privacy and security and that arguably have a nexus to technology and may need additional technology requirements or specifications to support them that we wanted to put before you in the hopes that we could make sure that if in fact a portal is the direction that the Meaningful Use Workgroup continues to head in and that's endorsed by the Policy Committee, we've got a portal that actually has the necessary technical functionalities to support privacy and security. Then, in terms of other policy requirements that don't really have a technical nexus, we've got a little bit more time to chew on those.

We've got three of them here on this slide number seven, that arguably are about privacy and security, and one is audit trail capability. We did mention this in some of our previous discussions but because we were really focusing on identity and authentication of patients for portals, we didn't really close that loop. So, we've got a draft audit trail capability needed, number one, and two others here, the need to have data provenance because the portal is not just view only. It's view and download, in accordance with the Meaningful Use Workgroup's materials that has been under discussion to date.

Then, the third one is one that I grabbed from the Markle Common Framework materials on their Blue Button Initiative, which has been launched by both the VA and CMS for their, you could call them portals, you could call them shared PHRs, you could call them tethered PHRs. I think there are a number of names for it, but they have added download functions to patient data views within EHRs. In the stead of consensus policies that Markle had developed was a desire to have a mechanism that an automated service that a patient might use, like a PHR, that would assist the individual in downloading data into a PHR. That it's better not to have a pathway into the portal that requires an automated service to use the individual's username and password in order to access it.

**Paul Egerman – Software Entrepreneur**

That's not the way I understood it, actually.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, I may not be explaining it correctly.

**Paul Egerman – Software Entrepreneur**

Maybe I got it wrong. I understood it that you could have automated pathways. They just had to be separate.

**Deven McGraw – Center for Democracy & Technology – Director**

No. That's absolutely right. It wasn't precluding automatic pathways, but they actually called for a separate pathway in order to avoid—because based on their findings and the stakeholder group that they worked with, if there was only one pathway then essentially for an automated service to be able to access that on a patient's behalf, they'd need the individual's username and password to ....

**Paul Egerman – Software Entrepreneur**

But they might need that also for the other pathway.

**Deven McGraw – Center for Democracy & Technology – Director**

Oh, all right, well that's not—

**Paul Egerman – Software Entrepreneur**

So, I just viewed it that they had two pathways. I didn't think they put in what's written here.

**Deven McGraw – Center for Democracy & Technology – Director**

Oh okay. That's my understanding. Do we have anybody from Markle on this call? Okay that's unfortunate.

**Paul Egerman – Software Entrepreneur**

These are the three, right? We only have three.

**Deven McGraw – Center for Democracy & Technology – Director**

These are the three. Just to let you know what was on the other slides, there was some other policies related to portal functionality that are more like usability issues. I included them on the slide only—they all came from the Common Framework document and I didn't want to necessarily leave them off, but it was our opinion on our co-chair calls in talking about this that these are not really privacy and security related. Again, they're sort of more usability issues that it's probably not really in our provenance to

decide but maybe ought to be moved over to the IE Workgroup. So, just to let you know what we have here. So, I'm going to go back to slide seven, Paul, and go ahead and make your point.

**Paul Egerman – Software Entrepreneur**

Well, let's go through them one by one. Let's start with the first one, which is basically there needs to be an audit trail of accesses to the patient's portal, and it needs to be accessible by the patients upon request, and it be included as stage two certification. So my question is, how to people view this? Is there controversy? Everyone looks at this and there's sort of like—?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

So, the underlying assumption is that patient portal is an EHR function?

**Paul Egerman – Software Entrepreneur**

That's right. What we're talking about here—Wes, good comment. The terminology is really confusing, and people use in a lot of different ways. When we say patient portal, we're talking about a view into the EHR system. At least for stage one, we're looking at this probably in a very narrow way. Some of these patient portals let you do things like make appointments or cancel or pay bills or something like that. This is just the ability for a patient to look and see what their lab results are.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Sid you mean to say stage two?

**Paul Egerman – Software Entrepreneur**

Yes. We meant to say stage two.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

So, we're looking at number one in the discussion now. Is that right?

**Deven McGraw – Center for Democracy & Technology – Director**

That's correct.

**Paul Egerman – Software Entrepreneur**

That's correct.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

No comment.

**Paul Egerman – Software Entrepreneur**

Okay. So, does no comment mean you're fine with this?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Yes.

**Paul Egerman – Software Entrepreneur**

Okay, so is there anybody who has a problem with number one?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Well, I'm kind of confused. We've had considerable discussion about patient portals and authentication of patient's in—to access their records. Where did all that go?

**Deven McGraw – Center for Democracy & Technology – Director**

Dixie, I separated that into the document that is the one called, on your downloads on the left hand side, and you also received it from ONC in your materials. I put all the stuff that I thought we were done with in one document so people would be able to focus on the things we hadn't done.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Well it seems to me then, if we're talking about—I'm kind of confused. If we're talking about patient portals, are we talking about this is a—well yes, it says—you were talking about patient portals as part of stage two right?

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, patient portals in a provider's EHR. We already have some recommendations that we put forward about—those guidelines on patient identity. Those are all in that other document. We similarly had some recommendations with some respect to authentication of patients, but that was as far as we got.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

All that is already in our stack of stage two measures.

**Deven McGraw – Center for Democracy & Technology – Director**

That's correct.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I see.

**Deven McGraw – Center for Democracy & Technology – Director**

I'm sorry if this feels like a very disjointed conversation. My apologies.

**Paul Egerman – Software Entrepreneur**

It's a good point, Dixie. So, what we did before is we first did user authentication. Then, we did patient authentication. Now, we're going a little deeper. We authenticated for this thing called a patient portal. Is there anything else from a privacy and security standpoint we want to say? So the first thing that we want to say, in addition to what we've already said, is there needs to be some audit trail capability to keep track of every time anybody, presumably the patient, accesses their portal and the patient needs to be able to see it in some way.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I would not limit it to auditing. I think auditing needs to be part of it, but I wouldn't limit it just accessing—there are other actions that you would want in the audit trail too.

**Deven McGraw – Center for Democracy & Technology – Director**

To deploy audit trails for the patient portals.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes. That's the way I would state it. Yes.

**Paul Egerman – Software Entrepreneur**

Say it again, Deven.

**Deven McGraw – Center for Democracy & Technology – Director**

It just would say, "Eligible providers and hospitals should deploy audit trails for a patient's portal, or in a patient's portal," so it wouldn't be limited to just access.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Or just say "should audit activities on the patient portal."

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, either way. You don't want to just have an audit trail program to just catch access.

**Paul Egerman – Software Entrepreneur**

Oh I see. Okay, so any other comments for that number one?

**Sue McAndrew – HITSP – Deputy Director**

This is Sue McAndrew. I apologize because I have not been privy to your prior conversation, so maybe this is just a point of education for me, but with regards to the portal—and this may go to the question of access or other things. Is this a unique point of contact that's definable, and what does it do other than pull information from the EHR and transmit it to who's ever at the other end of the view?

**Paul Egerman – Software Entrepreneur**

What you just described is what it does. It pulls information from the EHR and lets the patient view it, and the proposal is that they could also download it in some sort of a structured format. There's also a proposal that they somehow type in like an e-mail address or something and instead of downloading it in a format, it gets transmitted in a protected and defined format to whatever address is requested.

**Sue McAndrew – HITSP – Deputy Director**

But the download and other then the—don't give it to me send it here ... direction, it doesn't—there's no editing capability. There's no general disclosure capacity to others.

**Deven McGraw – Center for Democracy & Technology – Director**

No. Well, so if it has a download capability, it could grab, say it's a lab test result, and the portal that the provider makes available for them to view, they could download that and transfer it, disclose it themselves.

**Paul Egerman – Software Entrepreneur**

Yeah but—

**Sue McAndrew – HITSP – Deputy Director**

They download it on their own.

**Deven McGraw – Center for Democracy & Technology – Director**

That's correct.

**Paul Egerman – Software Entrepreneur**

Once the patient gets control of the data, sort of like the provider's off the hook, what happens from that point forward ....

**Sue McAndrew – HITSP – Deputy Director**

Right, this isn't setting up an intermediary personal health record that is still on the covered entity side of the portal.

**Deven McGraw – Center for Democracy & Technology – Director**

No, I don't think so, Sue. I mean, we're trying to scope out a set of policy requirements that would apply to a portal because that's what the Meaningful Use Workgroup is contemplating.

**Sue McAndrew – HITSP – Deputy Director**

How does it get the capacity to redirect this to a different e-mail address?

**Paul Egerman – Software Entrepreneur**

Again, the patient would enter it in—but it's been proposed; it hasn't been approved—the patient would enter it, somehow in the patient portal and request it.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Excuse me, I got lost. Where are we on the—?

**Paul Egerman – Software Entrepreneur**

Sue doesn't understand what a patient portal is. I guess we're educating—

**Deven McGraw – Center for Democracy & Technology – Director**

Which I don't mind doing, Sue, but we're a little pressed for time so is there a—?

**Sue McAndrew – HITSP – Deputy Director**

I'm just trying to figure out what kinds of functions would actually be audited and if in fact access—?

**Paul Egerman – Software Entrepreneur**

... you would audit any access to the patient portal.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Patient portals will include, among other things, being able to look up your lab results, may very well include ..., may include other interactions with— If you want to open up the discussion about the distinction between a patient portal and EHR we could be here until—

**Sue McAndrew – HITSP – Deputy Director**

No.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Okay.

**Sue McAndrew – HITSP – Deputy Director**

There was a question about whether access was too narrow. That the audit trail was just for access, and I was just trying to figure out—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Oh, as opposed to what somebody does once they have access to that.

**Sue McAndrew – HITSP – Deputy Director**

It seems to me that access is all that you would do ... portal.

**Paul Egerman – Software Entrepreneur**

There's access, there's download, there's transmit.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I think that's a very valid question then. Is what we're wanting to know is who logged in or are we wanting to audit what they did?

**Paul Egerman – Software Entrepreneur**

I think you want to know who logged in, when, what time, and what they did because it's a way for a patient to determine whether or not there's been any compromise, I suppose.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Okay so for use of a patient portal rather than access to a patient's portal would probably address Sue's issue.

**Paul Egerman – Software Entrepreneur**

I think that's right. Thank you very much Wes. So, I think hopefully we're in agreement with that one change for use of a patient's portal for item number one. Let's go on to number two. The patient portal should include provisions for data provenance. I think this is for data provenance when the data is downloaded or transmitted, correct?

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, well that would definitely be the most important functionality—

**Paul Egerman – Software Entrepreneur**

So it's written this way, I assume, because we're not really definitely defining all the aspects of what that might mean, but at a minimum, it would say this came from ABC Medical Group. It might have a date or

time stamp and a few other things, but it sort of says if you're going to download it there's going to be a certain amount of provenance information tells you—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

There are two points there, which I think are equally important. One, patient information being displayed through a portal should provide some provenance information to the user, to the patient who's looking at their data. The second is, information being downloaded should add provenance information. I'm on ABC's patient portal and I download my record and it's got lab results. It came from lab DEF, and a physician's note that came from ABC. That physician's note should say it came from ABC.

**Deven McGraw – Center for Democracy & Technology – Director**

I think that's right.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I think this is worded too open ended. I think it should be more explicit, like the data viewable through a patient portal should show the source of the data.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I agree with ....

**Paul Egerman – Software Entrepreneur**

I agree with what you're saying, Dixie, and Wes is saying, but I also want to keep in mind that we're the Privacy and Security Tiger Team. So my observation is, when you download or transmit the data, there's a reason to have some provenance information there. But why are we putting provenance information on the view, is that privacy and security?

**Deven McGraw – Center for Democracy & Technology – Director**

It's integrity issue.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I would say it is a privacy issue. I want to know where you got that information from. I wouldn't go so far as to mandate that it be displayed but that information should be accessible to the user. They may have to click on it. They may have to say something like send a message saying ... from, but the provenance should be available.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

It's more of a security data integrity issue than it is a privacy issue I believe.

**Deven McGraw – Center for Democracy & Technology – Director**

Right. Well, however you frame it I think it's—

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

It's important.

**M**

Integrity is part of security.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes.

**Judy Faulkner – Epic Systems – Founder**

Didn't we say earlier, I thought you said Paul that this was a situation, which was to view ... EHR, right?

**Paul Egerman – Software Entrepreneur**

That's correct.

**Judy Faulkner – Epic Systems – Founder**

You're not transmitting the data. You're not downloading ....

**Deven McGraw – Center for Democracy & Technology – Director**

That portal being proposed by meaningful use is view and download—view with a download capability.

**Judy Faulkner – Epic Systems – Founder**

Okay so you're talking about the ability to download that. Okay.

**M**

But even if you're viewing it, I think it's important—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I think we agree that both making it accessible while viewing and adding it to downloads are valuable functions. Paul has raised the question, I think—I'm inferring he's raised the question—we don't need to be that enumerative of options.

**Paul Egerman – Software Entrepreneur**

Yes. Basically, what I'm saying is we don't have to decide if it's got to have the date or the physician that ordered it, the patient or something like that. Somebody else is going to decide—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I would just leave it to the question of should we mention both accessing the prior provenance and adding to the provenance at download time at the level of detail that's appropriate for policy. I think it is just to avoid the very discussion we just had.

**Deven McGraw – Center for Democracy & Technology – Director**

Right, so, Wes, you're talking about framing this so it's clear that we're talking about both the ability to access provenance when you're viewing it, as well as to have provenance be with the data when you download it.

**Paul Egerman – Software Entrepreneur**

That's right. I understand, Wes, is the additional provenance is the providence of where the download comes from. So, this download is coming from ABC clinic and it occurs on April 5<sup>th</sup>.

**Judy Faulkner – Epic Systems – Founder**

So you're not saying that the lab portion of it, that these two numbers came from ABC lab, and that number came from XYZ lab and the radiology report came from Dr. Smith. You're not doing that.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I was doing that.

**Paul Egerman – Software Entrepreneur**

... not necessarily. Somebody might do that at some point, but we're not doing that.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Well, provenance is not a technically defining term, as far as I know, but the use in the art world, for example, is a thread of source back as far as you can trace something. So, I have been believing that a download of a—I mean, this is all PCAST stuff, right? A download of material from the Cleveland Clinic that included information that was provided by a referring provider in Arkansas, that included information that came from a lab in Arkansas to a referring provider should show all that information as far back as it is known. So, if it is not known how the provider got the hematocrit then it's not there, but the format should allow for it to be known and that should carry through.

**Paul Egerman – Software Entrepreneur**

Well, certainly it's a good idea to say that they might have to transfer information that they don't have. So, that part works really good. But the ... answer your question, Judy, is we're trying to be purposefully vague on this point, in terms of what is the actual provenance, because I think there's going to be a lot of other discussions about it.

**Judy Faulkner – Epic Systems – Founder**

Right, and I use a portal all the time. I think that when I get my lab test results, I don't care what lab they came from. I ... my clinic and they went to three different labs depending on ....

**M**

But you might care if you got an STD result that you didn't think applied to you.

**Judy Faulkner – Epic Systems – Founder**

Well, then I'd go back at that time, but I don't want ... up because 99.99% of the time, I've never had a situation where it doesn't apply to me. Let's say 100% of the time in all the times that I've looked at it, it's always applied to me. ... go through it.

**M**

Can I suggest one other thing though too, not only would necessarily the patient but other users who are accessing data want to ensure what the integrity of the data. Obviously, understanding the origins is important to a provider.

**Paul Egerman – Software Entrepreneur**

I understand, but we're only talking about the patient portal right here.

**Deven McGraw – Center for Democracy & Technology – Director**

But, we are in fact talking about if we're giving patients a download function and at least part of what underlies the reason for doing that is we expect the patients might actually go on and share that data potentially with other providers, then it makes it more useful.

**M**

Exactly. That's my concern ....

**M**

John Halamka's allergy example applies really well here. Well, I guess that's part of the data about the allergies ....

**Paul Egerman – Software Entrepreneur**

So, what we're saying is this item number two should have two points. The patient portal should be able to make available appropriate provenance information—we won't necessarily define what appropriate is—for viewing and download. The second point is when download occurs, it needs to add additional provenance to correctly identify information about the download or the transmission itself.

**M**

I agree.

**Judy Faulkner – Epic Systems – Founder**

I'm not sure I get— Explain them again Paul, please.

**Paul Egerman – Software Entrepreneur**

Okay there are two points. The first one is just says appropriate provenance when you view it, so ... what that is but an example just might be the date the test occurred or could be the date and the physician who made a diagnosis or ordered or did maybe a radiology interpretation. Somebody's going to define what that is, but whatever that is, is what we're saying is appropriate provenance is when you view it, and also when you download it. When you download the second part, is you have to add some provenance. What

you're adding is a ... simple thing. This says downloaded at 3:10 p.m., April 5, 2011 from St. Joseph Hospital. So you at least identify because you have two downloads and they're different ... first.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I think it's just as important to add that to say the data is available does not say it's mandatory to show it. To say that the data's available in a download implies nothing about how it will be shown. It just says it's part of the data ... part of the data ....

**Paul Egerman – Software Entrepreneur**

Are you okay with what I just said Judy?

**Judy Faulkner – Epic Systems – Founder**

I'm thinking of my own use for the system, and I just follow the system in use today and I'm thinking of— certainly I, as the patient, don't want to see a bunch of lab tests. I want to graph them but I can't even see to graph them because every lab test has who sent it, what time they sent it and everything and I can't even see the pattern ....

**Paul Egerman – Software Entrepreneur**

Yes ... to say appropriate because I agree 100% that I'm a patient I need to know the date that the test occurred, which is sort of like provenance, but I really don't care which lab did it because it's just information I want to see. In fact, it actually might confuse the hell out of me, because the sample was taken at my doctor's office, and I never heard of the laboratory before that ....

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Once again, I think we're ... two issues. One is the construction of the user interface for the patient portal and the other is the availability of data. So, I am not advocating that as a patient you have to look at all that data in order to find out what your A1c is. I am advocating that you should be able to get that information if you want it. You can take this issue about the patient only cares about a graph as terms of number and use that in designing your patient portal but it's just not something we're trying to regulate.

**Paul Egerman – Software Entrepreneur**

Yes and what I'm trying to say by saying appropriate is, is I don't want to have the argument right now or the discussion right now as what's needed or not needed. I don't know where that discussion goes. That's just a separate discussion.

**Deven McGraw – Center for Democracy & Technology – Director**

Right.

**Judy Faulkner – Epic Systems – Founder**

I'm trying to think that what we don't want to do is ruin the healthcare value that the portal brings to patients by having a view into important data for the patient to make decisions on and change his or her life on ... cholesterol, weight, all sorts of stuff that ... healthcare in order to—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Isn't that a user interface question?

**Judy Faulkner – Epic Systems – Founder**

Yes it is, but—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

But we're not regulating the user interface. Nothing in this recommendation says anything about what the user interface should look like.

**Judy Faulkner – Epic Systems – Founder**

It implies it though, I think.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

No, I don't think so.

**Judy Faulkner – Epic Systems – Founder**

It says if it is there, when you download it—

**Deven McGraw – Center for Democracy & Technology – Director**

It doesn't say that, Judy.

**Judy Faulkner – Epic Systems – Founder**

Well what are the words?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Paul said at one time, in a way, that it did use—say did could imply it had specified about the user interface, but I had been picking at those words over and over again to make sure that instead of saying you have to be able to see it, it has to be available just to avoid that issue.

**Judy Faulkner – Epic Systems – Founder**

Okay, if it says that, then I think we're fine. If it all implies that that's what the patient sees, then it's just—

**Paul Egerman – Software Entrepreneur**

I agree. We have to keep in mind that implementing these patient portals in stage two, it's a big step. I've had discussions with a lot of people about this and there's resistance to it. You've got some of the smaller EHR vendors saying this is a ton of work, you've got other people saying, ... we really want to do this. I think we want to do it, and so we've got to be careful that when we get started on this, we don't make this too big of a step because then we won't get it done. So we've got to be very sensitive to that issue, which is perhaps a long winded way of saying we got to be sensitive to the issue that Judy is saying. We want to make sure that we're not putting some restrictions on the view because that's where the value of the thing is, in terms of patients just want to see information.

**Judy Faulkner – Epic Systems – Founder**

Exactly.

**Deven McGraw – Center for Democracy & Technology – Director**

So, maybe it's actually better stated simply, which is to say that patient portal should include appropriate mechanisms for data provenance, both with respect to view and download, which need to be determined in subsequent discussions. Maybe we need to say needs to be ...—

**Paul Egerman – Software Entrepreneur**

... determined by the Standards Committee.

**Deven McGraw – Center for Democracy & Technology – Director**

—yes, within separate discussions that take into account both usability, functionality and the need for integrity. We're just trying to put a placeholder here and kick the can a little down the road. We'll probably end up with the can, by the way.

**Paul Egerman – Software Entrepreneur**

Well, I don't want the can. It's a different issue. You just got to be very careful when we say patient data integrity is a privacy and security issue because then we've got all kinds of stuff. We have to worry about the format for the result of the hematocrit because that's a data integrity issue.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Is anyone suggesting that we have to buy into the notion that data integrity is a privacy issue in order to agree on this point?

**W**

No.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

No?

**W**

No.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I have the rare advantage of being able to advise Paul that he's not sticking to the agenda, and we should move on.

**Paul Egerman – Software Entrepreneur**

You've been waiting a while to do that one.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I've been waiting since I've known you, Paul.

**Paul Egerman – Software Entrepreneur**

So, what do we do on two? Is it resolved?

**Deven McGraw – Center for Democracy & Technology – Director**

I think it's resolved.

**Paul Egerman – Software Entrepreneur**

Okay, let's move to three then. Boy, I'm just sitting here all red faced. Okay, so here's what's written here. What's written on the screen is portals should include mechanisms that prevent automated services from requiring individuals to provide username and password. So, what's written here is—and I think I know where this came from. I was in on a previous phone conversation where people have expressed concerns they didn't really want patients to have to give their username and password to their PHR vendor. To speak to that issue is I think there's nothing wrong with doing that. The way I look at it, it's the patient's username and password and they should be able to give it to whoever they want to, and plus you've got a situation, patients might have three physicians, they have five physician's offices they go to and each one has a different patient portal, a different username and password. If they can enter all that stuff into a separate PHR system and it can do a one-step download for them, that's a good convenience.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Isn't the issue here, whether they have to reveal it to the third party as opposed to the way it's done with Google Health and HealthVault right now, which is that you do separate—you do provide your username and password but HealthVault never sees it.

**Paul Egerman – Software Entrepreneur**

Yes I know. I think what your suggestion, Wes, is there's a basic structure for those two, which is a second double logon. You log on to your healthcare provider, you log on to them, and then you've got the connection. So, that would work really good with this download, upload structure. But there is another structure you could do where you give your—it's easier to think about if, instead of thinking about a HealthVault or Google Health, which is a web-based PHR, you think about it as a PC-based PHR. So, you've got your PHR system on your home computer, and you put your username and passwords into it. The reason why you do that is then on Friday or once a week, you say to it, check to see if I have any data, and it logs into every provider for you and does the download and sees if there is anything for you.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Well, Intuit has a financial system that's online that works the same way. You give it all of the usernames and passwords for all of your credit cards, all of your stock accounts, and everything else and it pulls data down, and I won't use it.

**Deven McGraw – Center for Democracy & Technology – Director**

That's why I won't use it either. It's admin.com.

**Paul Egerman – Software Entrepreneur**

Well, it's like that, but the way I look at that is, is that's a reasonable choice but it's the consumer's choice. In other words, that's not anything for us to deal with.

**Deven McGraw – Center for Democracy & Technology – Director**

Well, except, I think the reason why I put it on here is that at least with respect to Markel's Blue Button Initiative, they as a matter of policy said, there's a better way to do this, and ... some technical folks—

**Paul Egerman – Software Entrepreneur**

I read that differently. I want to get to that, but that's not what this says. All right, I don't understand how you even implement what this says—

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

If you do implement it, it's less secure.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I would argue that a slight change in wording would probably solve this. Portals should include mechanisms that enable individuals to use automated services without having to provide its username and password to the automated service.

**Paul Egerman – Software Entrepreneur**

How do they do that?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Just like HealthVault.

**Paul Egerman – Software Entrepreneur**

My separation of this is that it's up to the consumer whether or not they give out their username or password.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

The question is if you believe it's feasible—

**Deven McGraw – Center for Democracy & Technology – Director**

Not to force people into—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Not to force people to do it, then shouldn't the portal—

**Paul Egerman – Software Entrepreneur**

Why would you force it? Nobody's forcing anybody to do anything.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

If you can't use the service unless they do it, you're forcing them to do it.

**Paul Egerman – Software Entrepreneur**

You can't use the PHR service?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Right.

**Deven McGraw – Center for Democracy & Technology – Director**

Right.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We have two good examples of PHRs that don't require it.

**Paul Egerman – Software Entrepreneur**

Yes, but my question is what level of control do we have over PHRs?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We don't, but we have control over portals, and portals can either say we support this outside mechanism or we don't.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Right, the same argument goes that how can a portal prohibit Google Health from—what we have here is that they would prevent Google Health from doing something, and we'd have no control over that.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, so it's in artfully framed. I'll absolutely concede that, but I think Wes and I, I think are trying to make the same point, which is that if the portals only mechanism for allowing for the use of an auto download service is for the individual to give up his or her username and password, that's not a great set of choices for consumers. So we're suggesting that the portals have some sort of functionality or mechanism or set of policies that would allow for consumers to use an automated service where they wouldn't have to make that choice. Doesn't mean that consumers might not choose an option that gives up their username and password. We're not saying that's prohibited but it's been my understanding, and Wes you underscored it for me, that in fact there is a way to do this without forcing that choice.

**Paul Egerman – Software Entrepreneur**

I don't agree with the premise though. The basic issue is—let's look at an example, if I've got a program on my computer, that's my PHR system. What it does for me is it signs onto my three physicians, and it downloads the data. What's wrong with that?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I would say that, first of all, that program doesn't necessarily have to—the portal doesn't even know it's dealing with that program, depending on how it's constructed. But if you're saying that a patient portal should offer only one way to download data and that is the way that requires that the accessing program have the clear text username and password of the patient, I would say that's not acceptable. I would say it's not acceptable to say we will force consumers into having to either to do that or not be able to access data from the patient portal given that we know that there are alternatives that are feasible.

**Paul Egerman – Software Entrepreneur**

I'm totally confused. What are you saying Wes?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Let me say what I think you're saying first to make sure I'm not misstating it. You're saying that yes—you're acknowledging that there's a problem with giving up your username and password online, but you believe that there are, in fact, some programs that might be entirely based on your own PC where you would consider giving up, taking the risk that the program has some security ... on your own PC that would cause it to give it up, but you'd still say that if the consumer wants to do that, we shouldn't prohibit them from doing that.

**Paul Egerman – Software Entrepreneur**

That's right.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

So, so far, I'm not sure I entirely agree with you but let's stipulate that. Now, I'm saying the average consumer out there, for any one of the number of reasons, will probably have more options available to

them for PHRs that are cloud based than that are locally based, particularly when you get to consumers who really use smartphones as their main way of accessing the internet. I would not want to say that it's acceptable for a personal health record that the only way it can give up data—it's acceptable for a portal that the only way it can give up data to a personal health record is by receiving the clear text username and password.

**Paul Egerman – Software Entrepreneur**

Well, yes, but that's—we're already saying that's not acceptable because we said they have to have two mechanisms. They have to have a download and they have to have a transmit capability. So, ... portals have to do that.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

If you want to write something that says, it is acceptable to use, to give up personal name and password only on the condition where someone has that stored on their own computer where it's not given up on the cloud and you think that's important, that would be okay with me. Let's just say, we have to let any portal vendor say, either you go with the risk of the cloud vendor giving up your password or you use something on a PC. I fully intend to give up my PC and get a MAC someday. But I don't know that the program will be available for the MAC. I just think you're being unduly protective of a very small portion of the market here.

**Paul Egerman – Software Entrepreneur**

My question is what is the problem we're trying to solve?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

The problem we're trying to solve is to make sure that the portal function of a certified EHR has a function that's available for download of data that does not imply by the way the function works that the program that is requesting the download has access to the user credentials for the portal.

**Paul Egerman – Software Entrepreneur**

How do we do that?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Can I make a suggestion?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We just said how to do it, Paul.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I think you're in the weeds way too far. I think what we want to just say is that the portal should include a mechanism to enable a user to securely download their health information to a third party. Period. Because I don't think we're going to be addressing every single possible—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I understand your issue about the weeds Dixie, and generally I'm in favor of it, but I am concerned here about the interpretation of securely. If your sense is that the people who write the certification rules for EHR portals would not accept clear text transmission of username and password as secure, then I guess I'm okay.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I don't think they should. If a user has to—pretty much everybody knows that—if somebody asks you for your username and password, you're not supposed to give it out.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We've got one person here who's clearly defending that as an approach right now.

**Paul Egerman – Software Entrepreneur**

Yes, I am. I'm not trying to tell you what's right or wrong. But the way I look at it, first of all, is it's my username and password, I can do what I want with it.

**Deven McGraw – Center for Democracy & Technology – Director**

Of course you can. And I don't think we're talking about preventing you from doing something that some of us think isn't such a hot idea. We're just trying to get the portal not to be configured in a way that forces people to make the same choice that you're so ....

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

If they want to use this hospital for their services, and this hospital has a certified portal, they can't be told that that's the only way.

**Paul Egerman – Software Entrepreneur**

There's a missing communication piece here. The portal goes one direction only, right? I mean I know there's a few places where you can ... it, but for the most part it goes one direction. It gives EHR data to the patient. Now, what I don't understand is how you are proposing to implement this concept that you're trying to implement.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We have proof cases for it already that is the notion that it can't be implemented can't be presented at this point because it has been implemented.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

... authorization to send it to the third party, and that's required by law in fact, that's what's in .... If the patient authorizes you to send their information to a third party, then you need to do it electronically. But I would not get in the weeds of passwords and screen scraping. We don't allow any of that. Those are technical implementations. I think what we're asking for is that the portal be able to send a patient's health information to a third party with the patient's authorization.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I don't know that that's a portal function. As far as I know, that's an EHR inoperability function.

**Paul Egerman – Software Entrepreneur**

Well the portal ... request it. How it happens we don't care. It would be a portal function ... be to request it.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Functionally the portal needs to be—the patient needs to be able to do that through the portal. Therefore, the security issue comes up, and I guess I'm willing to just accept Dixie's securely, and let that issue be fought downstream. But boy if I'm on the call, that's going to be a hell of a call.

**Deven McGraw – Center for Democracy & Technology – Director**

Now, we would need to be better prepared for it, I think. The difficulty in trying to dive down into the weeds when we may not have all the people that we want to have on such a call. We might want to seek out some additional information ahead of time in order to really resolve that question. I'm in favor of Dixie's resolution, which is to say it has to be able to be securely downloaded to a third party authorized by the patient.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

That's fine. So is that then—do we even need it, then or are—?

**Paul Egerman – Software Entrepreneur**

....

**Deven McGraw – Center for Democracy & Technology – Director**

I think it's helpful to mention it, but it wouldn't be worded at all like it is right now.

**Paul Egerman – Software Entrepreneur**

So we would just say any downloads requested by the patient or any transmissions to a third party have to occur securely?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Well, no our portals should include mechanisms that enable secure download of—

**Deven McGraw – Center for Democracy & Technology – Director**

Yes. Good.

**Paul Egerman – Software Entrepreneur**

Okay, I don't have a problem with that.

**Deven McGraw – Center for Democracy & Technology – Director**

Anybody, else.

**Judy Faulkner – Epic Systems – Founder**

I'm fine with that.

**Deven McGraw – Center for Democracy & Technology – Director**

Well the remaining ones are not privacy and security related. They are, again, ones that I borrowed from the Blue Button download initiative. Four, five, and six on slide eight are usability issues that, I think in the interest of time, and the fact that we don't have a lot of background information on this to discuss it even if we wanted to, we probably should take those off the plate and then just sort of discuss with the IE workgroup who's responsible for dealing with some of these other portal functionalities but might be desirable but that are not privacy and security related. Then number seven is really about transparency and education of patients when they're opening portals. I indicated here on the slide that we really could and we can take this up later because it doesn't have the same degree of time sensitivity of all of the other things we've been doing because it's not tied to a technical functionality that we need to necessarily tee up for stage two certification.

Does anybody else want to add anything before we close off the portal discussion? Okay. Well, John, we have a little bit of time, was there something else, John Houston, that you wanted to mention.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

I decided not to.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, did we intimidate you?

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

No.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, that's right. That's not possible. Does anybody else have anything that they want to add before we move into public comment?

**Judy Faulkner – Epic Systems – Founder**

Back on the data at rest encryption, where it did talk about the data center, I thought last time we talked about this you said—and maybe I am just remembering wrong—that the main data center data did not have to be encrypted.

**Deven McGraw – Center for Democracy & Technology – Director**

Again, we're going to reframe this whole thing, Judy, so that it focuses more on what the HIPPA Security Rule addressable implementation specification is around the issue of encryption of data at rest and

asking for providers and hospitals to attest that they have addressed the particular data at rest specification as part of their risk assessment and not go into detail about what specifically they need to examine and that was my impression, that our consensus is really shaped around. We want to stick to what the rule already requires. We want to make sure the spotlight is shined on encryption of data at rest but not necessarily to specify with more detail because the institutions really are responsible for figuring that out. That's what it means to address an implementation specification.

**Judy Faulkner – Epic Systems – Founder**

Deven, is it your belief in understanding rules, that the data in the data center, the database itself has to be encrypted?

**Paul Egerman – Software Entrepreneur**

Let me do my best to explain that. It either has to be encrypted—tell me if I got this right Deven—or you have to have some plan for the security or explain why you didn't encrypt it.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, I think that's basically right. Dixie, do you want to chime in here?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes. An addressable implementation spec is a requirement in that you have to either implement exactly what it says or you have to argue your case for implementing something that is equivalent.

**Paul Egerman – Software Entrepreneur**

So the ... case could be is you've got other security, it's too expensive. There could be some argument that you make, but you have to— It's what the rule already says. We're not asking you to do anything new.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

It's like a mitigating control.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Exactly, you can't just say I've got this database that's out on my front porch and it's too expensive for me to encrypt it, so I'm not going to. You have to show that you have otherwise protected like put it in a room and locked the door.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Exactly.

**Deven McGraw – Center for Democracy & Technology – Director**

Sorry, it's an implementation specification for access control, right?

**Judy Faulkner – Epic Systems – Founder**

If putting in a room and locking the door is fine, then that's good. I think for many different systems, it's really response time issues of encrypting ....

**Deven McGraw – Center for Democracy & Technology – Director**

We want to be very careful that we're not going beyond what this security rule already provides. We're just shining a spotlight on this one provision.

**Judy Faulkner – Epic Systems – Founder**

Yes. I'm just trying to understand it because it's a huge issue if in fact what the security rule really does say is that it will have to be encrypted. However, if it is meaning that locking the doors is fine, then ....

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We're not saying one way or the other. We're simply saying that whatever CMS says.

**Paul Egerman – Software Entrepreneur**

And also, Judy, a lot of people look at this in terms of their operational system, but ... the problems appear to occur is in backup copies of the system. People still doing the backup copies on taped media for example, but even on hard media, that's a place where you could encrypt the backup copy and they're not and when they dispose of it the backup copies based on some disposable rule is when places are running into trouble.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Or when FedEx notifies them they lost their copy.

**Paul Egerman – Software Entrepreneur**

Yes.

**Deven McGraw – Center for Democracy & Technology – Director**

That's another one. Anyone else? All right, well folks this has been a super call. So, we have a call on April 18<sup>th</sup>, which is just after the Health IT Policy Committee meeting, we'll be able to report back on how we did. There may be some follow-up work that needs to be done based on questions that we might get from the Policy Committee, and if there is, we'll take the time on that call to do that. But if we don't have very many of them, then we're also going to use time on the 18<sup>th</sup> to do a little bit of a check in on where we are in the process of filling out policies for the nationwide framework and think about where we still have gaps, what have we not done yet, what do we need to get, which should we get to first. Do a little bit of planning for the next several months. So, it will be an opportunity for us to assess where we've come. The folks from MITRE are going to pull together some materials for us so we can see almost in one document a summary of where we've been. So we can chart a course of where we need to go in the future. Understanding that sometimes questions may come into us that we don't necessarily always have the ability to completely plan our work, but we're still going to try.

Paul, do you have anything that you want to add before we open the public comment?

**Paul Egerman – Software Entrepreneur**

Good meeting, spirited.

**Deven McGraw – Center for Democracy & Technology – Director**

They almost always are.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

We've been having a lot of those lately.

**Deven McGraw – Center for Democracy & Technology – Director**

All right, well Katelyn can you open the phone up for public comments?

**Katelyn – Altarum**

We do not have any comment at this time.

**Deven McGraw – Center for Democracy & Technology – Director**

Thanks everyone. Good weekend all of you and very much appreciate your time and attention.