

**HIT Standards Committee  
Consumer Technology Workgroup  
Transcript  
August 20, 2013**

**Presentation**

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

Thank you. Good morning everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Standards Consumer Technology Workgroup. This is a public call and there will be time for public comment at the end of the call. Please remember that the meeting is being transcribed and recorded, so please state your name before speaking. I'll now take roll.

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

Present.

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

Brian Carter? Arthur Henderson?

**Arthur R. Henderson – President – Affinity Networks, Inc.**

Present.

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

Brian Ahier?

**Brian Ahier – President – Gorge Health Connect, Inc. /Mid-Columbia Medical Center in Oregon**

Present.

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

John Ritter?

**John Ritter, MS – Software Engineer**

Present.

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

Anshuman Sharma? Susan Hull?

**Susan Hull, MSN, RN – Chief Executive Officer – Wellspring Consulting**

Present.

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

Mohit Kaushal?

**Mohit Kaushal, MD, MBA – Partner – Aberdare Ventures/National Venture Capital Association**

Good morning.

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

AJ Chen?

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**  
Present.

**Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator**  
Tonya Dorsey? John Derr?

**John F. Derr, RPh – Health Information Technology Strategy Consultant – Golden Living, LLC**  
Here.

**Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator**  
Yair Rajwan? Tom Jones? Liz Johnson? Christine Bechtel? Marcia Nizzari? Fred Trotter? Russ Leftwich? Holly Miller?

**Holly Miller, MD – Chief Medical Officer – MedAllies**  
Here.

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

**David Harlow, JD, MPH – Principal – The Harlow Group LLC**  
Here.

**Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator**  
Wes Rishel? Susan Woods? Kim Nazi?

**Kim Nazi, PhD, FACHE – Management Analyst – Veterans Health Administration**  
I'm here thank you.

**Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator**  
And we have Dixie Baker as a presenter. Is David McCallie on as well?

**David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation**  
Yes, I'm just joined.

**Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator**  
Thanks David. And are there any ONC staff members on the line?

**Ellen V. Makar, MSN, RN-BC, CPHIMS, CCM, CENP – Senior Policy Advisor – Office of the National Coordinator**  
Ellen Makar.

**Mary Jo Deering, PhD – Senior Policy Advisor, Office of Policy and Planning – Office of the National Coordinator**  
Mary Jo Deering.

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

Great. All right. This is Leslie. Thank you all for attending and today we have one agenda item, which will give us a lot of time to provide discussion and then also some recommendations going forward. As you know, each team has been assigned different work within the Standards Committee subgroups and the NwHIN Power Team, chaired by Dixie Baker and David McCallie, have made some very significant strides and far-reaching recommendations in the past few years, some great work. And today they're going to present to us some of the standards that are going to impact consumer exchange, get our feedback for discussion prior to going forward with their recommendation to the Standards Committee this week. So with that, I will turn it over to Dixie.

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

Thank you and thank you all for showing up on such short notice. We really appreciate it. As Leslie mentioned, we – the Nationwide Health Information Network Power Team developed some preliminary recommendations that we presented to the Standards Committee in June, so a few of you on the call have already seen this. And today we're going to – and we were tasked to run our recommendations by the Privacy and Security Workgroup and this workgroup. So, that's what we're doing today, what you'll see today, for the most part, are the same slides we presented to the Standards Committee, and where applicable, we will inject comments that the Privacy and Security Workgroup made. There weren't extensive comments with that workgroup, but where there were, we will mention them. David, did you want to mention anything?

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

No, but I want to warn you that I'm going to have to leave early, after about a half an hour, so you may be on your own.

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

Okay. All right.

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

Just a conflict that couldn't –

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

Well, it was a late scheduled meeting, so thank you for joining us for the first half. Next slide please. Okay. These are transport – okay, the task assignment, huh, are these the slides I sent to you yesterday? I thought I replaced that – the task that was assigned to us was to recommend any additional standards – to determine whether any additional standards were needed to support transport of data to and from consumers. And as you'll see at the very bottom of that slide, we interpreted, based on conversations we had with the ONC and further clarification that we got, that we interpreted transport standards to cover the broad capability of exchanging data, not in the narrow sense of just a wire between the provider and the patient basically. As I mentioned, we were asked to review these with the Privacy and Security Workgroup and this workgroup and to present our recommendations to the Standards Committee. Next slide please.

This is what you see before you are just a reminder. I think probably everybody on this call already has seen this or is familiar with this, but today, really the only transport standard that is out there for provider to consumer exchanges is the Direct protocol, the ONC Applicability Statement for Secure Health Transport. The HITECH Act called for capability of consumers to view, download and transmit information and only this – and to transmit it either to the consumer or to a named – third party named by the consumer. So the requirement – certification criterion to transport the health information to a third party named by the consumer is to be supported by the Direct protocol. Next slide.

Okay, what was – I may have just mailed the wrong slide deck, but what I have next here was we presented these recommendations to the full committee as preliminary recommendations at the June Standards Committee meeting. And at that time, the Standards Committee asked us to broaden the scope, to not be just specifically provider to patient or between providers and patients but to cover the broader area of any kind of transport, any kind of exchange of health information between entities that could be well served through a RESTful type protocol. For those of you who aren't familiar with REST, REST is really a style of programming, it's not a specific standard, but it's based on the standards that you use every day to access the Web through your Web browser, hypertext transfer protocol primarily. And so it's a very, very simple protocol that allows – that's specifically designed for accessing services on the Internet.

So the initiatives that the ONC asked us to look at in particular were the Blue Button Plus Initiative, which is what used to be called the Automated Blue Button Initiative, ABBI. Now it's called the Blue Button Plus Initiative. The HL7 new standard that's in development called FHIR, the Fast Healthcare Interoperability Resource and to look at a project that's co-sponsored by ONC and the Federal Health Architecture called RESTful Health Exchange. Next slide. Great. And when we looked at these three projects, there were some standards that kind of leaped out at us as being either common among at least two of them, or fit within a set of standards to support RESTful exchange.

You'll see all of them use HTTPS, which is Hypertext Transfer Protocol Secure, secure Web access, that's what you use when you go and buy something on Amazon or something. They all used another standard called OAuth 2.0 and OAuth is a way to authorize an application to do something. That's – you've probably seen this yourself when you might get a message up in front of you and it will say, LinkedIn wants to access your Facebook friends, let's say, and they'd ask you whether you want to authorize that or not. They're doing that using the OAuth 2 standard. There's an important difference between these three is that the Blue Button Plus Pull Initiative uses a registry concept that neither of the other two do, and we'll talk a little bit about that. The health content, FHIR of course is FHIR; Blue Button Plus Pull uses FHIR to query data and to retrieve selected sets of data from a provider. And then RHEX uses hData right now and is likely to transition to FHIR, so ultimately, they're all likely to use FHIR. The only one that uses OpenID Connect is the RHEX project. OpenID Connect is I guess the simplest way to describe it is it supports a single sign-on like capability between systems or organizations.

Next slide please. So in looking at the set, we noticed that there were – it was a mixed bag. There were – we had some lower level building block protocols, which I've just gone over, OAuth 2, OpenID Connect, hData and FHIR. And then there were a couple high level projects more than they were really standards, and that was Blue Button Plus and RHEX. So we decided to look at them in terms of these two levels of specifications, because they were really used for different purposes. The lower level were used to build a use-case based capability, which would be described as a higher-level protocol. Next slide, next two – next one. Okay.

OAuth 2, I mentioned that it is a standard for remote service and third party authorization. The important thing here is you're authorizing – we tend to think of authorizing individual users to do things, you know, a user is authenticated and after they're authenticated, they're authorized to do certain actions, like edit, to add to an EHR versus download an EHR. But in the case of OAuth 2, we're talking about authorizing and application, and in many cases, that application is a Smartphone app or an iPad app, but it authorizes it to do something. It's a flexible framework that has a lot of optionality in it. It's closely tied to Web technology and it's used here by both RHEX and Blue Button Plus Pull capability. It's a balloted standard and it's widely used by most of the major – by many of the major Internet companies. Next slide.

OpenID Connect is an OpenID Foundation standard for remote authentication and it passes the information about a user from a server that authenticates the user to another service so that that other service doesn't have to ask them to authenticate themselves again. Like I said, it's commonly called single sign-on. Another standard that does a similar sort of thing is SAML, Simple Access Manag – no, no, it's Security –

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

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

What is it?

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

I think it's Access Markup Language.

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

No it isn't Access, it's Assertion –

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

Assertion, yeah.

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

– Security Assertion Markup Language, SAML. We get to use the Acronym so much, but I'm trying to be clear here. Those of you who are familiar with the exchange protocol, it uses SOAP to access services and it uses SAML to pass security assertions between services. What we're recommending today, the RESTful protocol is analogous to SOAP, because both of them are ways to access services, and OpenID Connect is analogous to SAML. So, OpenID Connect is the successor to OpenID 2.0, it's layered on top of OAuth 2, so the two kind of go together nicely. It's an emerging standard, not as mature as OAuth 2, but it's growing and it's like I said, used for passing assertions. Next slide here please.

hData is a content standard, predecessor to FHIR and it's a way to expose healthcare resources. It really refers to the content being exchanged and its likely to be superseded by FHIR, so we won't mention any more about it here. Next slide. FHIR is a very exciting new standard that's coming out of HL7; it's kind of breaking new grounds at HL7 in a number of ways. First it's a very, very – it's getting a lot, in fact the majority of HL7 resources right now are going into the development of FHIR. It focuses on resources used for exchange and it emphasizes simplicity, implementability and human readability. So those – it goes without saying that it is – part of the specification is RESTful protocol for exchange, because it is focused on simplicity. The last point I wanted to make that makes it really different for HL7 is it does require a license, which is something I updated, it does require a license, but the licensing is free, free of charge, you don't have to pay the usual membership license to use it. Next slide please.

FHIR status, the base specification is complete and the team is currently defining resources. There – when I say the team, there's an enormous number of different organizations that are involved in the development of FHIR. In fact, CommonWell that David – Cerner Corporation is involved in has chosen FHIR for – to build its record, an encounter record locator service. They expect that it initially will be used for Web-centric social media applications, like those we've talked about here, but then it will probably – maybe – it will likely be used to exchange HL7 V2 messages to expose them with FHIR. Next slide please. Okay, moving on to the higher level, remember the higher-level protocol are composed – protocols are composed of using these standards that we've just gone through here, the building block protocols. Next slide.

The Blue Button Plus Initiative, I mentioned it used to be called ABBI, now it's called Blue Button Plus. And for Blue Button Plus Push, it simply adopts the Direct protocol that is already in the certification criteria and standards, so we won't talk about the Push from now on, we'll be focusing on the Pull, so all of the current efforts in Blue Button Plus today are going toward defining the Pull protocol as opposed to the Push. The Pull is an API that enables an application to pull EHR data, on behalf of the consumer. So you can easily see how this is – how OAuth 2 is ideal for what Blue Button Plus Pull was trying to do. So Blue Button Plus Pull allows an application or a Smartphone app or an iPad app to register using O – register with a provider using OAuth 2 and then after – as part of that, OAuth 2 will at that point ask the consumer is it okay for this application to access your EHR data? And the consumer at that point authorizes the access and all that is enabled by OAuth 2. It uses – Blue Button Plus Pull uses FHIR for searching for specific data objects and retrieval of those objects or resources. And it's RESTful, it uses HTTPS, it's a RESTful protocol. Next.

This is an example that we showed to the committee. It's a little bit confusing, in fact, I've tried to improve it in a later version, but you have three players. You have a consumer, you have an application server – an app, that the consumer is using connects to. And then you have an EHR service that is – will be a provider. So the EHR service is the entity that's the – the HIPAA entity, that's the entity that controls the EHR data. So in this picture, the consumer's using this app called My Health Monitor to record her diet history and blood pressure from a connected blood pressure cuff and all the data that she enters are uploaded to the My Health Monitor service. And most likely that's done over HTTPS, a secure Web link. My Health Monitor service then asks the EHR service – it registers with the EHR service and says I would like access to this consumer's record.

At that point the EHR service asks the consumer, shall we allow My Health Monitor to access your data, and the consumer says yes – if the consumer says yes, the EHR service goes back to the My Health Monitor service and says, okay, gives it a token and it allows it to access her data. The OAuth – all of this exchange and authorization is done with OAuth 2 and the query from My Health Monitor service, query of her health data and pulling her health data is done through the use of FHIR. FHIR, remember, is a content standard that has a query capability. Okay, next slide.

This is the page that I think you probably have seen before where you get your worki – you're doing some sort of thing, doesn't even matter. And all of a sudden you'll get a request for permission for an application, the application you're using, to access your LinkedIn or access your Facebook, or Twitter account on once you authorize it, that access happens. That's all done through OAuth 2. Next slide please.

Status of Blue Button Plus Pull is that the draft spec is available online. It responds well to this Internet use case where consumers control the ac – allow a third party to access their EHR data. The whole idea of whether you – whether the developers of these apps that are being authorized need to be certified or somehow proven that they are trustworthy is a debate that's going on, and I certainly – we would like to hear your thoughts on that. The Blue Button Plus concept now is that there would be something called a registry service through which an app would register, pre-register and say, I can protect my data, put me on the goo – the white list, make me a good guy. And the debate has two primary thrusts, I guess, maybe three. Number one is what really constitutes trust. Number two, is that – that obviously will require a whole new infrastructure that doesn't exist today. And the third is really is the process through which they would go to really prove their trustworthiness. At least at the time we put this together, which was in June, EHR vendors were currently under-represented in the development of a Blue Button Plus Pull; hopefully that has improved since then, I'm not sure how that is. Do you know David?

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

No, I don't have any statistics. I think the issue is that most of the vendors are deep in the middle of their Meaningful Use Stage 2 certification and they're all focusing on the Push requirement, rather than worrying about the future possible Pull requirement. So it's a prioritization thing.

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

Um hmm. Okay, next slide please. Okay, this is REST. And the purpose of REST was just really as an exercise to apply open-source Web technologies to demonstrate uses of RESTful, secure, standards-based exchanges. About – well, 2011 the NwHIN Power Team recommended that ONC support the development and definition of a RESTful transport alternative to the Direct protocol and the SOAP protocol that are in the standards today, so this project is directly responsive to that. The four standards used are secure Web HTTPS, OpenID Connect, OAuth 2 and hData, which as I mentioned, is likely to be – to ultimately be FHIR instead. Next slide.

The RHEX project has completed two pilots and is now – now has new pilots underway with the DoD. The new pilots are sharing images between the DoD EHR system, AHLTA, and third party provider systems. The – during the first phase of implementation, the Maine HealthInfoNet used the RHEX standards for transporting volumes of data to and from a statewide repository, and now they're implementing RHEX – those RHEX standards statewide for small and federally qualified health center providers. Next slide please.

The – I think that Leslie has shown you this graphic that was developed by the NwHIN Power Team I think in 2011, perhaps, but the intent is to use it to help assess when a standard is ready to become a national standard. And on the X-axis, the bottom, we have adoptability, how easy it is to adopt the standard. On the Y-axis we have maturity. And each of those criteria – those attributes, maturity and adoptability is further broken down into specific criteria and specific metrics used for really measuring how adoptable a standard is and how mature a standard is, and I think that Leslie has provided you with that document. So we put the red – what you see in red on here are the standards, those lower level protocols and the little white – the white boxes are projects.

When a project – when a standard is proven to be highly adoptable and mature, sufficiently mature, it then can become a national standard. Now this is – this evaluation approach was never intended to be kind of a pass/fail type of thing. The ONC asked us to do this to give them an input into their decisions on where to really invest in standards. It would tell them when a standard was ready for – but it was just important to tell them where do we really – what do we really need to pay attention to and get ONC people to support so that it gets – becomes more adoptable and more mature more quickly. And as you can see, of the standards we talked about in that lower level protocol, the Web HTTPS is – it's used everywhere. OAuth 2 is used just about everywhere, so it's quite mature as well. FHIR and OpenID Connect are those that are least mature and are least ready for national standardization at this point. Next slide please.

So the overarching conclusion of the Power Team was that HTTPS, OpenID Connect, OAuth 2 and FHIR together form a set of standards that are safe to use as building blocks for more complicated healthcare applications. I would add that the Privacy and Security Workgroup added an IHE profile called Internet User Authentication, IUA, that is built using OAuth 2 and it just constrains OAuth 2 so that it's more standard and more usable – user friendly for exchanging security assertions within environments for – that currently use SAML. And so we've added that to this recommendation, but not as one of the main players, but as, if you use SAML assertions or if you exchange security attributes in your environment already, you should look at this IUA profile as – with respect to its applicability to your environment and whether it would help you implement OAuth 2. Next slide.

We recommended that the ONC support and encourage this Blue Button Plus Pull, FHIR and RHEX, because we think they are all valuable efforts, and they've already made valuable contributions, but they really deserve support from ONC. But there's an important difference between Blue Button Plus and RHEX. Blue Button Plus actually has a potential, because it's responsive to a very specific use case, so it really has the potential of becoming an implementation guide that might be identified in a later version of the standards and certification criteria. RHEX, on the other hand, is very broad with a lot of flexibility and is best as a demonstration of these standards of how you can use these standards together. But because it's so broad, it probably is not a good candidate for a standard implementation guide itself. FHIR is very likely to become the next generation content standard for healthcare, so, I think we just have to watch, but there are a lot of resources going into it, including resources from ONC. Next slide.

I already went through that one. Next slide. Our next steps were to present these to the Privacy and Security Workgroup and this workgroup, so, I think we're ready for discussions or questions or comments.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thanks Dixie, appreciate that. And I'll take the chair's prerogative and ask some questions. One of the things that this group has mentioned is how do we describe an experience for a patient who wants to participate in all of these things. And I think that's work that could be something this group might take on, but have you had in any of your experiences the discussion about, okay, now we have these standards, what does this mean to the patient or consumer? How does the workflow happen? How do they achieve this? Has that been discussed at all?

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

Well, no. I think – no, not really workflow.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Okay.

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

The use case – I mean, we're a technical –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Right, I know.

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

– group, so we really don't talk a lot about operations and policies and that kind of thing. But the use case for Blue Button Plus is pretty clear. Blue Button Plus Pull, I'm talking about, well both of them actually –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Yup.

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

– but it doesn't really constrain the workflow for doing that, but the use case itself is that a consumer would want to use an application to – and allow that application to access his or her EHR data. And they would do it through the Blue Button Plus – using the Blue Button Plus protocol, which would need to be implemented in the provider's environment. And that's – but that's not workflow, that's really use case.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Okay.

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

Dixie?

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

Leslie –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Yes.

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

This is David. I'm going to have to drop off the call unfortunately, because I had a prior conflict due to the scheduling – late scheduling of this. But I'll just comment from the vendor perspective that, I mean I think that the Blue Button model, both the Push and the Pull obviously center around the provider's portal and the relationship that the provider will establish with his or her patients using the portal. So the Push model is obviously required for Meaningful Use Stage 2, we don't know if the Pull model will make it into Stage 3 or not, but I think that the focus point of the engagement will be around the notion of the portal, be it Push or Pull or ideally, in some future state, both Push and Pull. So, there are many other consumer engagement possibilities, but this particular set of standards and particular profile is really focused on the portal. So I think that's good and bad, I mean, the portal is not the be all and end all, but it's a critical step towards improving that data flow.

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

This is Wes Rishel. I wonder if I could just add something to what David said.

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

Yeah/

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

Sure.



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

So I think when we say the focus is on the portal and we think about the consumer experience, it's not too hard to look ahead and say, well, the portal experience may not be what happens on a laptop or on a desktop computer, it may be what happens on a Smartphone. It may be an app that is used both to access the portal and to access whatever the other app is that the patient is using. And this is the technology; if you look at where everybody has been and where they're headed; these are the technologies – the underlying technologies that the developers of apps and sort of browser-based, computer-based things are using. And while we haven't sort of identified a number of very attractive, specific use cases and talked them through, I think there are some important points to make.

One is that the experi – that the underlying mechanism here is that the patient authorizes the link between two applications using passwords or whatever – however they identify them. There's no direct – there's no involvement of a third party to make that and there's no automatic creation of these links. That people are familiar enough with creating those links now to understand both the upsides and the downsides of doing it, because these links are being used by Facebook. I mean, if you ever used HealthVault and linked your Walgreen's data to it, you were going through what appears to the user to be the same process. And I think that – my – and I'm a diabetic and I recently had my blood sugar, my A1c's go from an area where I was – I needed to begin to pay serious attention to my lifestyle and medications and stuff. And I went out and I bought a FitBit and I bought a glucometer and I bought a blood pressure/respiration cuff and it was easy to get them operating. And I tried to get somebody else's glucometer working with help 12 years ago and it was hard, and the reason was, that from the device to the cloud was all one vendor and then the interaction came between the cloud and another cloud app, or in this case, between the cloud and a doctor's office app.

We are using both the concepts that consumers understand generally and the mechanisms that the vendors in that milieu are heading towards in developing. So I think it promises any one of a number of – I mean I could easily imagine that I could tell my doctor, well I want to – go to my doctor's app or portal and say, all right, get my sets from FitBit and get my food log from MyNetDiary. And put that into your program that runs through and alerts you for care gaps and begins a care coordination session with me, if I'm not reporting or my blood sugars are up, or any one of a dozen other specific ways of imaging how these resources could be used together.

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

Thank you, I think that's a great overview of why these recommendations are powerful.

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

Leslie?

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Yes.

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

I want to add one point to what David – just for clarification because it's this group. The users – the provider's portal is the linkage point but I think that a lot of people think, when they think of portal, they think of a website, right? And what we mean by portal is a user – a consumer account that is the entry point for a consumer into a provider organization. So when OAuth 2 asks an individual to authorize a Smartphone app to access their EHR, they don't then suddenly see a portal page, right? It's just that they don't need a separate account, that authorization in OAuth 2 will use that same portal account to allow the user to check off yes, that's okay. Okay? So they don't get like all of sudden here I was using my Smartphone app and all of a sudden I'm back at my user's portal, that's not what we mean.

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

No, and this is David. Good clarification, you need a portal account for all this stuff to work and that's the point of identity proofing and account assignment that occurs. You might never, as a consumer, ever actually log into the portal page, but you're going to need a portal account, at least the way these are structured now.

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

Yeah, I think they'll just perceive the portal to be this app that they're using –

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

Right.

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

Or to be – I mean at some point, they will have had to create a login for –

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

Right.

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

– the portal account –

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

Yeah.

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

– and they may have done any – I want to also emphasize that this technology is not limited to EHR interactions.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Um hmm.

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

So, for example, I can personally recommend MyNetDiary as a great food-logging app for diabetics. It has special logic for dealing with fiber and sugar alcohols and carb counting. I mean, it's really – and it's very easy to use, it's a great app. But, I would dearly love to be able to get my steps from FitBit and my weight from My Electronic Scale from Withings in there. I can do that because those three vendors have made a deal, but it would be much easier to get a lot of vendors in the sort of the personal wellness or the personal disease management space to interact, if they had a single standard based on the technologies that they're used to using anyways. As opposed to having to adopt a technological approach that is more suited – or historically widely used, but not sort of at the edge of where they're developing now.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thank you.

**Holly Miller, MD – Chief Medical Officer – MedAllies**

I'd like to go back a second to something that David brought up –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

That's Dr. Miller I think.

**Holly Miller, MD – Chief Medical Officer – MedAllies**

Yes, thank you, I'm sorry. So Dixie, I really appreciate the OAuth 2, because to allow a consumer to access or to get into another system, I think that's fabulous, and then to have the consumer really control where they want to put their data. However, David brought up – identity proofing that has to happen and this is something that I think I'd really like Dixie to ask you about that. Because right now, in most organizations, when a patient signs up for an EHR-linked portal, there is that face-to-face identity proofing with a valid ID that has to happen. And so, in considering all of this, at what level and when does patient or consumer identity proofing happen so that it kind of sets all these wheels in motion.

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

Well I think that – obviously identity proofing is very important and establishing the level of assurance that you need for identity proofing –

**Holly Miller, MD – Chief Medical Officer – MedAllies**

Critical.

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

– right, it's policy, that's not technology. And that's exactly the kind of question that needs to be asked to the Policy Committee and the Privacy & Security Tiger Team. We try very hard to limit our work on the – I know in the areas of Privacy and Security in particular, it's very easy to just kind of get into policy, because policy drives it all, right? But we are not the body to specify level of assurance for identity proofing, that is a policy question.

**Holly Miller, MD – Chief Medical Officer – MedAllies**

Okay, thank you Dixie.

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

Dixie, can I add to that?

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

Um hmm.

**Holly Miller, MD – Chief Medical Officer – MedAllies**

Is that David?

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

No, this is Wes Rishel again. I want to make it clear that the technology supports whatever policy we need –

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

Right.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Um hmm.

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

– so she's not saying, oh, we haven't thought about that, she's saying, each of these places where you as a consumer have an identity, has a policy for how they identify you. Most of the places that consumers use, you are identified as the person who bought this product, if it's a blood pressure cuff, or you're identified as the person who created your food diary, but your identity is not proofed. The places where your identity is proofed right now are your electronic health record, for example, where the processes are typically you can't get on until you've been seen in the doctor's office or you've got a bill in front of you that's got a number on it that's not known to the general public. There are various ways of doing identity proofing, but it ends up, they know you as a patient.

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

– when they give you your portal, your portal account.

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

Right.

**Holly Miller, MD – Chief Medical Officer – MedAllies**

That's what I – that there is a face-to-face valid ID, identity proofing.

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

Yeah, but as far as –

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

Yeah.

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

– yeah, yeah. And what this process does –

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Can I ask you something?

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

Okay, is that AJ? We can barely hear you.

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Yes. The portal account is normally actually happens in the process of OAuth 2. So when we usually say OAuth 2, usually it actually includes user authentication on the, say the EHR portal.

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

But authentication is different –

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

But that's –

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

– authentication – we're talking three different processes here. There's identity proofing in order to get an account. There is authentication of a user with an account at the time that user needs to access the account. And there's authorization, that's also done – the authorization is done ahead of time, but when they ask for a resource, the system mediates the request and either gives it to them or not.

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Yes.

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

When I say – and Wes made a really, really important point, the technology that we've described here supports all of those, but the identity proofing, which is a process done to give a person an account, is a policy issue. The level of – whether they have to appear in the doctor's office and present 14 pieces of identification with a picture on it, that is a policy question. But once they're given that account, moving on to authentication, OAuth 2, that's where the portal comes in. OAuth 2 includes authentication of that person to the portal, as part of the technology. That's a technology issue –

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

Yeah.

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Yes –

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

– deciding the process –

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

– I understand that.

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

– for giving the account is not.

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

(Indiscernible)

**Holly Miller, MD – Chief Medical Officer – MedAllies**

And I guess my only – emphasize the importance of identity proofing as we open the doors of the kingdom.

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

Well I think it's important –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

AJ has – another comment, too. AJ?

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Yes, I understand all of that. What I want to say is that OAuth 2 plus authentication is a normal process that actually has a capability to covers all the priva – all the usual needs of privacy, including the authentication and authorization. But that's very – there's no – on the technology side, there's no missing piece there, that's – so there's no problem of covering the authentic – user authentication or face-to-face authentication. I want to add something on top of this overall use case, it seems to me the use case may actually drive – thinking.

What I want to emphasize is that the Blue Button Plus Pull mechanism or, I would like to call it simply BB Plus API mechanism is not only capable of – for doing the exchange between patient tools and EHR, in fact, its capable to make the exchange between the EHRs. And I'm actually doing some testing right now, I'm doing implementation of the BB Plus API and use that implementation to actually verify – to actually try to accomplish the test in the Meaningful Use 2 that's required for the VDT and also other – there's only five or six tests that are required in certification. And my initial – my current understanding is that in fact we can easily use the BB Plus mechanism to actually help the EHR vendor and providers to meet the Meaningful Use 2 requirements related to those patients's documents exchange.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

It's a good point, oh, go ahead AJ.

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

And the one question I have in my mind, the biggest question is that it will be terrific if we have a second mechanism for the EHR meaningful use certification. And the question then comes, is it possible, or is there any discussion now, that the ONC will consider that the BB Plus mechanism as say a second transport mechanism for the Meaningful Use 2, 2014 certification? Because I think that has a major – that could have a major impact in terms of adoption or implementation of the Meaningful Use 2 certification type of requirement.

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

Well, the 2014 edition, the final version of the standards and certification criteria is already out. And as David was pointing out earlier, all the vendors are busy developing systems to conform to that, so I'm certainly not a government guy or an ONC person, but I don't think it's very likely at all that it would make it for 2014.

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Okay.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

But AJ, you do bring up a good point in that this – the mechanism that's been described here could certainly be a framework for consent and interoperability for any application, including EHR-to-EHR and giving the patient the opportunity to provide those kinds of consents is a new thought in healthcare. To do it easily –

**AJ Chen, PhD – Chair, Data Committee – National Partnership for Action Region IX Health Equity Counsel**

Yes.

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

– with things that patients already understand and technology that's already pervasive, is in itself a great incentive for quick adoption. So I think that the recommendations, if we go back to that – the maturity index and we see how far up the recommendations are, that in itself I think will push for broad adoption, as well as Meaningful Use 3, in that potential recommendation. So –

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

Well remember, Blue Button Plus, it's not on that ready –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Right.

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

– in fact, they're still defining it. But there certainly is nothing that would prohibit AJ or anybody else from using OAuth 2 to implement a particular application or capability. I mean, it doesn't have to be in the certification criteria to use it, but the server that your app is asking permission of, has to support OAuth 2 for that to work. So, both ends have to support it.

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

Can I ask –?

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

I'm mindful of our time and we have to also have public comment. So I think we have time for about two or three more questions.

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

This is Wes.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Okay.

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

Can I just address – we started talking about identity proofing and then –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Yes.

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

– moved away from it, can I come back to that topic?

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Sure.

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

I'd like to be clear that none of this technology that we've discussed today discusses identity proofing –

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Um hmm.

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

– and in fact, once identity has been proofed, or if your policy is not to require identity proofing, and I'll come back to that, then all of this technology makes everything work afterwards. And I'm very concerned that we don't go overboard on identity proofing and to make that case, right now, one of – so a prototype of what we're talking about is HealthVault. And, as far as HealthVault concerns, I can be Foxy Lady 235 as my identity on HealthVault, and I can be Charles Atlas Strongman on Walgreens and there is no problem, because I'm the person who made the link between those two identities. Neither one of them checked my driver's license, neither one of them did – looked me up in a phone book, asked me what address I used to live at 25 years ago or all the things that people do to try to link a user ID to a real person's identity.

Same with all of the different apps I use now as a diabetic. I didn't have to go through – I didn't have the inertia of going through those steps to get started. I think that we know that healthcare providers have a different situation. They need to do identity proofing, very often that falls out of their process because they – first thing they do when you come into the office the first time is get your driver's license or something like that. And then they can reflect that in their systems. But I think it's important to recognize that when the user is authorized on two systems and creates a link, that's the user's intent. As long as we know they were authorized on both systems, we don't need to – we don't necessarily need to have both systems have a common method of identity proofing. Each system sets the level of identity proofing according to its legal and ethical requirements.

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

I think that's a really good clarification and what I see is the struggle will be with the provider's understanding of that and policies around how to release information and what their level of trust and association with the application assigned will be. So I think we've got a lot to go, but this gives us a good framework.

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

As the Consumer Workgroup, I hope you and we, because I'm hoping to join this group, will advocate for the consumer as the one who's able to control where their data goes, rather than the provider having – setting up great impedance to the data flow, based on his legal concerns.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

I think that that's a great comment. If we look at history and we see how power and control has shifted, it's often shifted by who controls the movement and I think your point is well taken for consumer advocacy. Michelle, I think we have a minute left and this has been a great discussion. I'd like – we didn't hear from a lot of the members, so I'd like to see if we could keep some agenda item open for our next meeting to further this discussion, but I'd like to turn it back over to you.

**Public Comment**

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

Thanks Leslie. Operator, can you please open the lines for public comment?

**Ashley Griffin – Management Assistant – Altarum Institute**

If you are on the phone and would like to make a public comment, please press \*1 at this time. If you are listening via your computer speakers, you may dial 1-877-705-2976 and press \*1 to be placed in the comment queue. We have no public comment at this time.

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

I'd like to thank this group for meeting with us today. We appreciate it.

**Leslie Kelly Hall – Senior Vice President, Policy – Healthwise**

Thank you Dixie, you guys have done amazing work and it shows all the time. Thank you very much. All right, with that, I think we're adjourned.