

**HIT Standards Committee  
Privacy & Security Workgroup  
NwHIN Power Team  
Transcript  
July 29, 2013**

**Presentation**

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

Good morning, everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Combined Health IT Standards Committee Policy and Security Work Group, and the NwHIN Power Team. I will now take roll. Actually, this is a public call, and there will be time for public comment. Please remember to say your name when speaking for the transcript. I'll now take roll. Dixie Baker?

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

Yep, I'm here.

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

Walter Suarez?

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

I'm here.

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

Chad Hirsch? Dave McCallie?

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

Here.

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

Ed Larsen? John Blair? John Moehrke?

**John Moehrke – GE Healthcare**

Yep.

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

Lisa Gallagher? Sharon Terry?

**Sharon Terry, MA – President & Chief Executive Officer – Genetic Alliance**

Here.

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

Peter Kaufman? Tonya Dorsey?

**Tonya Dorsey – Blue Cross Blue Shield, South Carolina – Chief Implementation Architect**

Here.

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

Leslie Kelly Hall? Mike Davis?

**Mike Davis – Veterans Health Administration**

Here.

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

Then the Power Team people I didn't call, Arien Malec? Cris Ross?

**Christopher Ross – Mayo Clinic – Chief Information Officer**

I'm here.

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

Keith Figlioli? Josh Mandel?

**Joshua C. Mandel, MD, SB – Boston Children's Hospital – Research Scientist**

Here.

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

Keith Boone?

**Keith Boone – GE Healthcare**

Present.

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

Wes Rishel?

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

Here.

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

Jitin Asnaani? I'm sorry; if you're here, can you pronounce the name for me?

**Jitin Asnaani – AthenaHealth**

Sure, I'm here, and it's Jitin Asnaani. You got it just about right.

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

Okay. *[Laughter]* Thank you. Ollie Gray?

**Ollie Gray – Department of Defense**

Here.

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

Are there any ONC staff members on the line?

**William Phelps – Policy Analyst – Office of the National Coordinator**

Good morning, Michelle. Will Phelps.

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

Good morning, Will.

**Ellen Makar, MSN, RN-BC, CPHIMS, CCM, CENP – Office of the National Coordinator**

Ellen Makar.

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

Hi, Ellen. With that, I'll turn it over to Dixie.

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

Okay. Thank you, and thank you all for joining us this morning. I think this is a really important meeting where we'll be reviewing some other, a set of recommendations for standards that the Nationwide Health Information Network Power Team recommended through the Standards Committee at the June meeting.

The goal of this meeting is to gain consensus to get the Privacy and Security Work Group support for these recommendations. As you'll see, the recommendations came out of or were motivated by several initiatives that the NwHIN Power Team reviewed. The intent is not to go back and review in detail those initiatives, but really to focus on the standards that were recommended instead.

I realize this is a bit, may be a bit confusing because I chair both groups and Dave McCallie is my co-chair on the NwHIN Power Team and he's also on the Policy Committee Workgroup, but we'll try to keep it clear that when we're in whichever, the two respective roles. David and I will go through the presentation that was given to the Standards Committee in June and then we'll, that will be followed by the discussion of the set of standards that were recommended. We request that you hold questions until we finish going through these slides. The intent of the slides is to show you the recommendations, how we got there, and briefly address these pictures. Following that presentation, we're fortunate to have Debbie Bucci and Justin Richer and John Moehrke, who will be helping us with the discussion as they all three have some really good, solid experience with these standards that we recommended. I also want to thank William Phelps and Debbie Bucci for their help in preparing this meeting. With that, David, do you want to add anything?

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

No, I think that's a great summary. This is a terrific group. I think it should be a good discussion and hopefully we'll have some pretty smooth sailing here. I think there's a lot of consensus and convergence, but we need to make sure, for the sake of the broader Standards Committee mandate.

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

Walter, do you have, would you like to say anything before we start?

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

No, I'm—this is Walter, I'm looking forward to the discussion. Maybe during the conversation, Dixie and David, you might want to talk about the relationship, perhaps—I don't know if this was covered, but the relationship of the recommended standards to the very thoughtful evaluation criteria that was developed by the NwHIN Power Team as well.

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

Yes, we will cover that.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

That's great; thank you.

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

We also will cover, there was kind of a change in scope at the last, when we did present these recommendations to the committee, so we'll also mention that as we go through the slides.

Okay, with that, would you—Caitlin, would you advance the slides, please? Okay, just go to the third slide is good. Okay.

The task that was assigned to the NWHIN Power Team was to recommend whether ONC should consider enhancing the current portfolio of transport standards, specifically to support consumer exchanges for Stage 3 and beyond. In Stage 2, you'll recall, they added the Direct protocol to enable a provider to download an EHR to an individual so that the current standards that are there are, the Direct protocol is required and the exchange SOAP based protocol is optional. They asked us specifically—ONC asked us—to specifically consider the Automated Blue Button Initiative (ABBI), the HL7 FHIR initiative, and the RESTful Health Exchange, and so you'll see that those were really, reviewing those three projects were really the foundation for the recommendations, and they asked us to present our recommendations. In reviewing the assignment, we interpreted transport to be more than just transport standard, but rather the conveyance of EHR from a provider to a patient and vice versa.

Next slide, please. These are just the standards that exist today. On the left, you have the Patient Empowerment Requirements that appear in the 2014 edition of EHR certification criteria, and on the right, you'll see what I mentioned there is the ONC Applicability Statement for Secure Health Transported. It's the only one that is required for Stage 2 or 2014 Meaningful Use. Securely sending messages requires authentication of the patient and the EHR technology and the FIPS 140-2 encryption.

Next slide, please. Okay, these are the three, the ABBI, the Automated Blue Button Initiative, the name of that initiative has been changed to the Blue Button Plus Initiative. I have a link there to the S&I Framework Initiative that's now called the Blue Button Plus. The HL7 Fast Healthcare Interoperability Resources specification, I have a link there that's called FHIR. The third one is the RESTful Health Exchange, which is a project co-sponsored by the Federal Health Architecture and the S&I Framework; there's a link there. Those are the three initiatives that we were asked to look at.

Next slide, please. As we reviewed these three, we had some really nice presentations on all three and we noticed some commonalities emerging from these standards. As you'll see, all three of them use HTTPS, Hypertext Transfer Protocol Secure, which is the standard that's used for RESTful Exchanges that are secured using Transport Layer Security, so they all three use a RESTful Exchange, a Secured RESTful Exchange. All three use another standard called OAuth2. There's a slight difference between the three in that Blue Button Plus Pull uses, well, recommends a registry of certified applications, and we'll talk a little bit about that in a minute when we get into more detail about Blue Button Plus Pull, and OAuth2 for FHIR is suggested but not required. Then the healthcare content, two of the three, FHIR and Blue Button Plus Pull use FHIR as their content standard. The RHEX standard uses hData, but is likely to transition to FHIR later on.

Next slide, please. So what emerged from our discussions were two layers of protocols. There was what we call the lower level protocols or building blocks, which were OAuth2, OpenID Connect, and hData and FHIR, which is what we just went over. Then at the higher level protocols are more of the composite protocols which were Blue Button Plus Pull and the RESTful Health Exchange or RHEX. So FHIR really is a lower level standard. It's not really an initiative associated with specific use cases as are Blue Button Plus and RHEX.

Next slide, please. We're gonna look at each of these, lower level standards first and then the higher level protocols after that.

Next slide, please. Okay, OpenID Connect. OpenID Connect is an OpenID foundation standard for remote authentication. It is an alternative, it's very similar to SAML, which is used in exchange in a traditional SOAP web services stack. OpenID Connect enables the sharing of security attributes associated with a RESTful Exchange. It's designed to replace OpenID 2.0 and it's layered on top of OAuth2, another standard we'll be talking about here. Right now, it's an emerging standard in a limited but growing use and in here, in this presentation, it's used by the RHEX initiative.

Okay. Next slide, please. hData is a predecessor to FHIR, the HL7 content standard, and it's for the RESTful exposure of health resources, where everything is considered a resource. It is an HL7 draft standard for trial use and it's likely to be superseded by FHIR, because HL7 is putting a lot of effort right now into FHIR as their next generation content standard.

Next slide, please. FHIR, which is the Fast Healthcare Interoperability Resources, is a new HL7 standard, and it's strongly supported by HL7's leadership and it's rapidly emerging as industry, as a next generation HL7 content standard for the industry. It focuses on resources for exchange. It defines a very simple structure that is based on the RIM. It's mapped to the RIM, but the RIM doesn't need to be computable. It allows for extensions that are formally published, formally defined, it defines how you define extensions and the narrative explaining how the standard is used. It has a strong emphasis on simplicity, implementability and human readability. It includes, the spec itself, includes a RESTful transport, although other transports can be used. Then there's new, for HL7, it really requires a license. You have to sign a license with HL7, but you don't have to pay for that license, so that license you use free.

Next slide, please. Okay, this is the status. It's complete. The spec is complete, and now the HL7 primary effort is going into defining resources and they have specific plans for 25 CCDA resources, definitions, and six IHA and DICOM resource definitions. They're targeting around 150, and at that point, they will—these are basic resources, and at that point, they'll shift to defining profiles that use multiple resources. HL7 expects that the initial use will be in web centric social media apps and then they expect it will be the replacement for version 2 HL7 messaging where FHIR will be used to expose HL7 v2 content. Then they expect to ultimately replace the CDA Release 3 with FHIR. In this exercise, it was used by the Blue Button Plus Pull initiative and also CommonWell, which is an initiative that a couple of our members, Arien Malec and David are associated with, selected it to build a record and encounter locator service.

Next slide, please.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

I think you skipped slide nine by virtue of the next slide, which is the one that explains Open Auth.

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

Oh. You know, I thought I did when it got—would you go back, yeah, I think it comes before OpenID Connect. Thank you. Yeah, I don't know how we missed that one. OAuth2 is the one that's used by all there of these, and it's an IETS standard for remote service and third party authorization.

It's important to note that authorization for OAuth2 is not what we usually think of as authorization in terms of authorizing a user to do certain things. Its focus is really on an individual authorizing an application to take certain actions, and we'll give you an example in a minute. It is a flexible framework with lots of optionality and so it does need to be profiled for specific use cases. It's closely tied to HTTP or REST, and it's used here by both RHEX and Blue Button Plus. It's not used by FHIR, it's RHEX and Blue Button Plus Pull.

Yeah, so that would be the standard, it's widely used by major Internet companies like Google and Facebook and eBay and LinkedIn, and we'll give you an example. Thank you, Walter.

Okay, now let's catch up. Okay, now we're going into the higher level protocols.

Next slide, please. Blue Button Plus includes two protocols, one for pushing information from the provider to the consumer, and the other for enabling an applicational consumer to pull information. Blue Button Plus is the next generation Blue Button, which I think most people are familiar with. Its focus is on consumer access to their record, both Push and Pull. This exercise, the Push, which is pushing from the provider to the consumer or to a third party named by the consumer is, for 2014, requires the use of Direct. The initiative itself just adopts Direct for Push, and most of the effort—all of the effort right now—is going into defining Blue Button Plus Pull, which is what enables query of an EHR for an individual's record. It would enable a user to authorize a second provider or a personal health record to actually query for their information.

The Blue Button Plus Pull is an API that enables this pull of EHR query and pull of EHR data. It uses OAuth2 to register to enable an application to register with a provider. It uses FHIR for the content search and retrieval, and it uses secure REST for the actual transport itself. It allows open registration, which is no prenegotiated vetting of the application and it also allows registration of the applications, preregistration.

Next slide, please. This shows, I hope, what Blue Button Plus Pull, an example of what it would do. As you'll see, what we have here, we have a consumer who has a smartphone, and on that smartphone, they have an application, a software application called My Health Monitor app, and the smartphone is also connected to a blood pressure cuff. The consumers using this application, My Health Monitor app, and that app reaches out to the EHR service and says, "I want to pull some information from their EHR," okay? The EHR service, the provider would have an OAuth2 enabled server there, and that server would be able to understand the OAuth2 query from the My Health Monitor service, so it would go over and say the My Health Monitor is asking for access to the EHR. The EHR service would then go back to the consumer and say, "Do you allow this? Is it okay with you if this My Health Monitor accesses your EHR?" and the consumer would be given a little screen on their smartphone that would say, "Do you authorize this or not?" Then if they do, then the OAuth2 authorizes the My Health Monitor app to pull data from the EHR using FHIR and REST.

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

Dixie? This is Wes.

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

Uh huh, yeah?

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

That interaction identified by the dashed arrows, do you anticipate that happening each time My Health Monitor requests access to the EHR, or is that something that sets up a relationship?

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

That is a policy decision, that's not a technology decision. That's something that's specified by the service provider, whether they need to authorize it every time or just can authorize it once and then six times, whatever, but it's not—it's a policy decision, not a technology constraint.

**Keith Boone – GE Healthcare**

Just to clarify, Wes, it is possible that you can set up a relationship that is sort of a persistent, authorized relationship, and as Dixie points out, your policy can determine how long that relationship can be used before it has to be re-verified, including it could just be a one-time only relationship, and that's enabled by the technology, but the policy would figure that out. This is Keith.

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

Yeah, this is David. Think of it, Wes, like the way Twitter clients work with the Twitter service. Some of the re-authenticate you into Twitter every month or so, and some of them don't.

**Keith Boone – GE Healthcare**

Yeah, I'm just trying to compare this to some of the products that are out there being used now.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

Are we—this is Walter—aren't we equating authentication with authorization in this case? In other words—

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

No.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

Okay.

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

No, this is authorizing an application.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

This is the consumer saying, "Yes, I authorize," but somehow before that, the consumer was authenticated by the system, right?

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

Yeah, but the consumer is not who you're authorizing. You also have to authenticate the application, but that's a separate list. Let's go ahead and get into the authentication as well. What this is doing, the point of this slide is that this is not authorizing an individual, it's authorizing an application to do the pulling.

**Male**

Okay. Dixie, I hope you address this later on, but sort of my concern is any implication that the smartphone has to be available online to represent the consumer every time My Health Monitor wants to go to the EHR service.

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

No, it does not. It does not.

**Male**

That's, the dashed arrow is, what other agent represents the consumer side of those dashed arrows, other than something running on the smartphone?

**Joshua C. Mandel, MD, SB – Boston Children's Hospital – Research Scientist**

This is Josh. I think I can give a quick clarification on this one. The user is online and authenticated for an up-front ... that generates a token. The token has an expiration date that's set by policy, but once that token is generated, it can be used by the app, even by the app's back end server for as long as it lasts without the patient being on line.

**Male**

So the arrow, the dashed arrow is representing generating the token?

**Joshua C. Mandel, MD, SB – Boston Children's Hospital – Research Scientist**

Yeah, the up-front token generation step.

**Male**

Okay, thank you.

**Joshua C. Mandel, MD, SB – Boston Children's Hospital – Research Scientist**

Yeah, there's some arrows—there's some missing arrows, but if you put all of the flows in place, it would be unreadable. *[Laughter]*

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

Yeah, one iteration actually had the tokens in there, and it really did get, *[Laughter]* get a little messy, but yeah. Yeah, and let me show you this—go to the next slide. I think this will, I think the next—yeah, I think will explain it to you. Because I think, I suspect everybody on this call has seen this, where you're using LinkedIn or you're using Google Plus, and all of a sudden you get a message as you're using that application and it says something like, "Here," it says, "My Health Monitor is requesting permission to do the following." It asks you, the user, to authorize the application.

Now, if you're using a smartphone, it doesn't send this thing while you're not using the phone. When you bring up LinkedIn or you bring up Google Plus, it will then appear because it knows you're using the service, and it'll say, "Okay, this other service is trying to access your Facebook data. Do you want to let it access your Facebook or not?" and at that point, you authorize it, and as Josh pointed out—

**Male**

Yeah, no, I was just hoping to see that the previous diagram was consistent with the workflow implied by the slide, that's all.

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

Oh, so it's not all clear?

**Male**

Yes.

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

Okay. Okay, thank you. Next slide, please. Okay, the draft specification Blue Button Pull is available online. It defines very well defined use case that fulfills the requirement of consumers controlling who to expose their data to. Obviously, this standard is very, Blue Button Plus is particular amenable to the type of mobile apps that people use these days.

Blue Button Plus is still having conversations about whether these apps need to be precertified before they can be registered with a server. In other words, if I write an app and I put it up on the Apple store and people download it, does that app need to be certified ahead of time? Now, this is one of the questions that I'd like to see this group discuss today is, how much confidence do you have, is needed in these apps that are made available through Blue Button Pull?

In the Blue Button Pull, it was pointed us that the EHR vendors are currently underrepresented. I understand since that time more have joined the Blue Button Plus Initiative, but it is important that EHR vendors be represented, and certainly—

**Keith Boone – GE Healthcare**

Yeah, Dixie, this is Keith.

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

Uh huh. Hi, Keith.

**Keith Boone – GE Healthcare**

I think the biggest issue is not the representation of EHR vendors, because I know of several who have been involved, including myself, in that activity. It was more so being able to get data holders who are involved to be able to do the piloting of the work.

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

Okay. Is this Keith Boone, or—

**Keith Boone – GE Healthcare**

Keith Boone, sorry.

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

Okay. We have two new Keiths, but I'm glad you're able to join us today, Keith, thank you.

Okay, next slide. RESTful Health Exchange—REST is not itself a standard, but it applies commonly known web technologies to access resources in a very simple way. The RESTful Health Exchange is an initiative out of, that was sponsored initially by the Federal Health Architecture and jointly was coordinated by the ONC. It applies, these RESTful tools, to enabling access to health information. The REST initiative was directly responding to an earlier NwHIN Power Team recommendation that, where we said that we have an e-mail based protocol in Direct, we have a SOAP based protocol in Exchange, and there was a need for a RESTful protocol and the RHEX initiative was begun. It's layered over core Internet standards including HTTPS, OpenID Connect for authentication, and OAuth2 for authorizing applications, and it used hData for health content.

Next slide, please. The status of the RHEX initiative is that they have completed two pilots and they're starting on other pilots this year. Ollie Gray from our NwHIN Power Team is on today and she's been involved in these pilots with Patrick and brought the team forward. Debbie Bucci, who's also on the line, and Justin Richer, who also is on the line, I hope, also were involved in RHEX—very heavily involved in RHEX.

There are new pilots underway at TATRC, the one having to do with the sharing of large images, and the other is providing patients access to their medical history.

**Christopher Ross – Mayo Clinic – Chief Information Officer**

Dixie?

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

Yes?

**Christopher Ross – Mayo Clinic – Chief Information Officer**

This is Cris. Can you just tell me what TATRC and AHLTA are?

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

Oh.

**Ollie Gray – Department of Defense**

Dixie, this is Ollie.

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

Thank you. *[Laughter]*

**Ollie Gray – Department of Defense**

TATRC is the Telemedicine and Advanced Technology Research Center. We're with the Department of Defense and we do medical research. AHLTA is the electronic medical record for the Department of Defense.

**Christopher Ross – Mayo Clinic – Chief Information Officer**

Great. Thank you so much.

**Ollie Gray – Department of Defense**

You're welcome.

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

Thank you, Ollie. I was having a mental block on the TATRC acronym. TATRC is Fort Detrick. They do, yeah, the medical research. The state of Maine is implementing the RHEX statewide. They did a pilot in 2012 and now they're implementing it statewide with, to support small independent providers and the federally qualified health centers in underserved areas. There's also a planned pilot with the VHA, the Veterans Health Administration; that one's easier than TATRC.

Next slide, please. Okay, here is the assessment that Walter referred to earlier. The, I guess it's probably a couple of years ago now—one of the first things that the NwHIN Power Team did, and was asked to do, resulted in the development of a number of some metrics and criteria for evaluating when a standard was ready for prime time; when it was ready to be considered to become a national standard. The two main axes that the standards are evaluated on is adoptability and maturity. On this slide, we have all of these, the two initiatives, the Blue Button Plus Pull, is still, is Emerging Standards. It's highly adoptable, but it's not really mature; it's still in development.

The standards that we're really focusing on are in red, here. HTTPS, every one of us uses it every day, so it's definitely ready to become a national standard. OAuth2 is certainly widely used and there are pilots underway like the ones we just talked about with RHEX, pilots underway, and with FHIR as well. It's still, the base standard is fully developed, but they're developing resource definitions and piloting it, CommonWell being one of the early adopters of FHIR. OpenID Connect is still being defined.

Next slide, please.

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

Dixie? I had a couple questions on the video slide—this is Wes. If they can bring back the previous slide, it would help me, thank you. Just, what do we mean when we say a pilot? Do we mean something that is operated by real providers with real patient data, or do we mean something more circumscribed than that?

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

The pilot wouldn't—you know, remember when we discussed this in the NwHIN Power Team, we had a long conversation whether, about whether we were talking about maturity within healthcare or outside of healthcare. Pilot I don't think is limited to healthcare, it's more the maturity of the standard.

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

Let's change that to real consumers or real users with real data or—I'm just trying to understand the difference, I understand the pilot is a conclusion rather than an input to the slide, but I'm just trying to get a sense of what we're thinking about is a demo or a Connectathon on a pilot or is it, is pilot sort of the next stage in our thinking where we're talking about committing to actually using it to get the job done?

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

Well, see, we—you'll recall, Wes, because you're on the time—we defined very specific metrics for maturity. I'll be happy to send that to everybody or send you the link to it, but no, Connectathon definitely is not up at the pilot level.

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

Yeah. I think it's an important step, it's just not, in terms of our assessing readiness, it's an intermediate point. Then I—I guess I'm wanting to confirm, recall the process, and I may not have been at the meeting, where we put FHIR at the moderate level in that what I hear sort of on the FHIR list server and so forth seems to make it seem like it's a little more in a sort of a stage of spontaneous or rapidly adopting change, which I think it needs to do, and I don't want to constrain it. I'm just trying to understand how we got to this current positioning.

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

Right. Let's save that for our discussion—

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

That'd be great.

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

- and let's [*Cross talk*] our comments right now to just specific questions to make sure you guys understand what—

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

Yeah. That's fine, thanks.

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

- all right, but we definitely will put that on our discussion list, here.

Okay. Next slide, please. Oops, you went up to—okay, this is really an important slide. [*Laughter*] I'm glad we didn't miss this one. This is the overarching conclusion, is that the Power Team concluded that Secured RESTful transport (HTTPS) plus OpenID Connect for authentication, OAuth2 for authorization, and FHIR for representing healthcare content could together be used as a safe and appropriate set of standards to use as building blocks for more complicated healthcare applications. That's really the recommendation that our goal is focused on today.

Okay, let's go to the next slide, please. I want to get through these and get into the discussion. Okay, the NwHIN Power Team recommended number one, that ONC support and encourage the development and piloting of Blue Button Plus, FHIR, and RHEX. We also noted that the Blue Button Plus Pull focuses on a very specific identified need to enable to a consumer to access their own health information, and to authorize a third party application, whether it be another provider's application or whether it be an application on their mobile phone to also access that EHR. We felt that FHIR was highly likely to become a key next generation content standard for healthcare. There is a need for a FHIR based CCDA, and that's currently being developed.

Next slide—ooh, I think it's our final one. We felt that RHEX was a useful demonstration of how these standards could be used together to support robust, simple health exchange, but we felt that it was—and it's proving to be true, they're doing multiple pilots—RHEX itself is too broad to become a standard. Blue Button Plus we felt was narrow enough in its use case that it could be a standard. RHEX really would need to be, is a good demonstration of how these standards can be used together, but itself is broader than what we would want for a national standard.

Okay. We also recommended the replacement of hData with FHIR. Is there anything—I think that's the end. David, is there anything more you want to add?

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

No, I think that's good. There are a lot of details which I think will come out in the conversation around what things need to be profiled above and beyond the kind of core standard. I think some of the stuff that John has for us and other parts of the discussion will touch on that, because I'm betting we don't have a lot of dispute about the broad recommendations here and it'll come down to the details of specific profiles, you know what I mean?

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

Yes, I agree. We don't we, we've asked Debbie Bucci and Justin Richer, who have worked on both the Blue Button Plus Pull as well as the RHEX Initiative, to talk about some of the security questions that their teams encountered and issues they discussed and conclusions they reached in putting together those two standards.

I know we also have Josh Mandel on the phone, and Josh briefed us on Blue Button and has also been highly involved in Blue Button Plus, so maybe the three of you could discuss what are some of the security questions that you undertook, your teams undertook to address during, while you're putting together these initiatives and what conclusions did you reach, why did you reach them?

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

Dixie, this is Walter. Could I ask a very quick classification question?

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

Yes.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

These are recommendations to adopt these standards; are they for Meaningful Use Stage 3, I presume, is that right?

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

Well, we really didn't, we weren't specific on that, but your question brings up another point that I meant to point out. When we presented these standards to the committee, the full committee, they—and we had noticed it ourselves that there's no reason why these standards should just be used for consumer communications. They could be used for any instance where you really want an application authorized to access a record. The Standards Committee recommended that, going forward, we extend this recommendation to include consumer communications but not be limited to consumer communications. It's not, we're really talking about a set of standards that allow RESTful Exchange of health information, period. However, we did not specify a particular addition for Meaningful Use. We were really talking about, in the ordinary day to day, how do we facilitate and enable the sharing of health information.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

The timeline is an important question, because it just—I mean, right now, we are about to start Meaningful Use Stage 2. I don't know how adopting a new, or a set of standards, in this case for secure transport, would affect the implementation of Meaningful Use Stage 2 already or is this something that is to be done for Stage 3.

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

That will come out of the maturity exercise. I think when it comes time for the Standards Committee to address Stage 3, what are our recommendations and standards for Stage 3—which we haven't, we aren't yet—I think then we'll discuss whether they're ready. This discussion, I think we could get pretty bogged down in Stage 2 versus Stage 3 versus Stage 4, et cetera. I think what we really want to do is determine whether we think these are on the way to becoming—and back to Wes', where it falls into that matrix I think is highly relevant, but I really don't want us to get backed into Stage 3 or Stage 4 or Stage N.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

No, no, I didn't mean to go, veer the discussion, I just wanted to understand if there was any discussion done about it—

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

Yeah. No, no.

**Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

- but we can move ahead. Thank you.

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

No, we haven't discussed Stage whatever at all.

**Christopher Ross – Mayo Clinic – Chief Information Officer**

Dixie?

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

Yeah.

**Christopher Ross – Mayo Clinic – Chief Information Officer**

This is Cris. To Walter's point, if I look at your slide 23, I think your recommendation is that ONC supported and encouraged development and piloting, which seems to me—Walter's point is an excellent one, but it seems to me as though the recommendation is really orthogonal to Meaningful Use. This is suggesting that ONC continue to advance these standards. I think we can do that without making a statement about Stage 2 or 3.

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

Right. Exactly right. Yep.

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

This is Leslie, Dixie, and I just think that relative to that is, do we have to make any comment at all about existing standards that have been recommended for Meaningful Use 2 that would be impacted by this? Is there any sort of unintended consequence where we've promoted a particular group of standards and now we've changed, or is there enough compatibility that that is not relevant?

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

Well, I think—

**Keith Boone – GE Healthcare**

This is Keith. I'd love to speak to that.

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

Yes.

**Keith Boone – GE Healthcare**

I think we're looking at, to me, as I read this, this is a both-hands recommendation. In the work that I've been doing on Blue Button Plus with FHIR, a lot of that involved demonstrating how the query parameters in the Blue Button Plus Pull RESTful API are mapped back to metadata that it shows up in the direct specification and in the NwHIN Exchange specifications and, in fact, the prototype that I had developed really is using some of the base IHE, XCA, and XDR specifications from NwHIN Exchange on the back end. I think, from the impact, I think we're looking at something that is just simply a different view on the same base set of metadata and queryable content.

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

I often think that—I would like to repeat our recommendation that we made about at the end. That is, we did assert that the Blue Button Plus Push and Pull, but Push already is a standard, was much narrower and already, just by definition, it's more amenable to becoming a national standard than RHEX is. Because it's a very well defined use case. David, was that you I heard?

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

Yeah, no, I'm just agreeing that, I think these are forward looking. We were asked a forward looking question; we were not asked to go back and challenge the things that are already set in regulatory stone for Stage 2. I think we are kind of essentially addressing two questions. One is, are these protocols in general suitable for healthcare and are they adequately profiled, et cetera, and then the implication of that would be, as certification standards emerge for Stage 3 and beyond, should these protocols be a part of those certification standards? We weren't specifically asked to address that question, but the Stage 2 regs are written, so I don't think—we didn't do any looking backward.

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

Right. Okay, now—

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

I was just simply—this is Leslie again—I was asking that simply because the vendor community has often said, “Don’t change your mind. Give us something to work on.”

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

No, no. We're not changing.

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

It sounds like this is very compatible with existing work and just simply perhaps easier, so *[Cross talk]*.

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

Yeah. If you look back at our assignment, it was additional standards. We weren’t even asked to look at what’s already there.

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

I mean, it—this is David again—it always complicates life when you add things to the table, but so be it. Technology moves forward.

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

This is Wes, Dixie. If you want to constrain this conversation, you can cut me off, but I just want to make a general statement that we have, we're sort of between two forces, here. One is, every time we go into the formal process of setting a stage, we have by definition a very limited time horizon, and we have a specific requirement to be up in the upper right hand corner of the grid.

This is, I would interpret this as being what Farzad would call eyes on the star, feet on the ground. It’s an attempt to introduce more radical change in technology that you can do in those incremental bites, and at some point, ONC will have to make a decision whether to bite the bullet and go forward. We will advise them, but at that point, they’ll have to balance the risk of whatever is new being relatively untried, at least in healthcare, at least in the United States versus staying with the little nibbles on the existing standards.

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

Right, and what we've been asked to do is to give them our advice—you know, if you, for example, if this team wants to say, “We think, ONC, you should put more pressure to do more pilots for Blue Button Pull,” let’s say, we should say that. I’d like to—let’s see, it’s 10:00. I really want to get into this ... Justin, Debbie—

**Debbie Bucci – Office of the National Coordinator**

Hello. Can you hear me okay?

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

Yes, hello. Yes, can you hear me?

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

Yes.

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

Excellent.

**Debbie Bucci – Office of the National Coordinator**

Okay, great. I'm just gonna take a few minutes and really hand it over to Justin, but my experience, I come from NIH, I come from outside, really, healthcare. I started with the database access with the username and password that, when somebody would sign on, that made sure ... password that wasn’t enough, that you added Mutual SSL and it should, there’s a whole thing about authorization to the services, whether it’s web or not, it’s just a natural migration. As we knew from that, when I left, by the time I left NIH, I was working on a cross agency access to create profiles to be able to apply for grants based, pulled from multiple sources, using OAuth, and then watching OpenID, which isn’t secure enough, but it was OpenID ABC that was using OAuth baby version 10.

I just watched this mature along the way when I got to ONC, and where my specific interest is in REST is at the federal level, the FICAM level. I was pressing for both an OAuth and OpenID Connect profile for the federal government so that when healthcare says, “Yes, go forth,” they were talking about the profiles that the federal government could look at the name on. We did a lot of work, Justin came to the group working with the ... Federated Integrated Working Group, and we compared those profiles to see how close they are, and then also very closely watching Blue Button efforts. I'll just drop it from there and hand it over to Justin.

### **Justin Richer, MS – Lead Technologist – MITRE Corporation**

All right, yes, so everybody, my name is Justin Richer, I'm actually with the MITRE Corporation supporting ONC here. What I've—my background here is that I've been a part of the working groups that have been defining OAuth2, its various extensions, and OpenID Connect. Actually, just a very quick update to the slide, there—OpenID Connect is now in a voting period to have the implementers' draft accepted, which means we will see a final version of the specification in the next couple of months. That is moving along towards a full final spec very quickly, now.

Anyway, you guys have gotten a nice overview here of what all of the different technologies do and what we did with the RHEX project was really just try to bolt everything together in a real system and move data around to see, kind of tease out what worked and what didn't and what was underspecified and what we had to kind of say what do here and there. Some of those things that we found were that OAuth2 is fantastic as a framework and it gives you all of the bits and pieces that you need to build lots of different kinds of systems, but in order to build RHEX and have it be truly end to end interoperable, we had to nail down some of the mayas to shoulds, and the shoulds to musts, and sort of things like that from the OAuth specifications into what we ended up writing as a RHEX profile for both OAuth2 and OpenID Connect.

Those things included things like the client must use a client secret and it must have a certain level of entropy, which the server can check. You must use a signed token format. The OAuth itself doesn't actually care about what's inside the token itself. With the RHEX profile, we actually specified what's inside the token so that all the various players can actually look at the token and figure out, kind of, “All right, so where did this come from? Should I trust it? What should I trust it for?”—that kind of stuff we actually specified outside of, or inside our RHEX profile of OAuth2. Overall, it was really just a matter of picking from the shopping list of available technologies and available best practices. We didn't really have to invent anything to solve the RHEX use cases that we were actually using. We were able to use off the shelf stuff.

Now, with Blue Button Plus, I can say that we were almost able to use everything off the shelf; the main difference there being the preregistration and sort of the trusted registration of the clients. The good news there, and kind of the interesting story, is that the Blue Button use case and the work in the Blue Button Working Group is actually directly pushing back into the OAuth working group inside the IETF, which is the Internet Engineering Task Force; that's the standards body that defines the OAuth and its extensions. Blue Button is itself actually influencing the future direction of the standards that it's using, because it is a very valid and a very powerful use case to be able to say, “We have lots of different authorization providers, lots of different data providers, and lots of different data consuming applications that are both provider facing and patient facing.” It creates a really rich ecosystem for the technology to actually grow in.

Even with that small bit of invention, we were able to actually fit that very easily inside of everything that's already been defined. All of the Blue Button stuff that we have to sort of make for this special case actually builds directly on top of all of these open protocols as it is. You can actually use a Blue Button, what's called an open registration client, and that will work with completely, absolutely standard IETF, off the shelf OAuth components, and that will function. I think that that's a testament to not only all of these building block protocols, their flexibility and their utility, but also kind of their elegant simplicity, if you will, in that they solve their small sets of problems and solve them very well in a way that can be adapted and reused by lots of different use cases.

Also, as Debbie mentioned, I've been involved with, from time to time with the FICAM, or the pending—or impending depending on how you look at it—FICAM profiles of OAuth and OpenID Connect. I think that the work here that we're doing in the healthcare standards space can really push those FICAM style profiles and recommendations forward, because this is a very concrete set of uses of all of this technology. Because as all of you have probably figured out by now, you've realized by now, this OAuth and OpenID Connect have actually nothing to do with healthcare on their own. They weren't invented for healthcare, they weren't developed with healthcare in mind, particularly, and electronic healthcare records just—it wasn't really a consideration with either of the protocols. They're much, much broader in their scope and in their reach.

I think that what we're doing here with using these in the context of FHIR as an access protocol that needs to be protected by OAuth and by OpenID Connect. Blue Button, as the ecosystem of all these different systems and the way that they interconnect with each other, I think that this is getting us a very compelling and concrete cornerstone upon which we can build some very solid general recommendations that will help not only things like Blue Button, not only healthcare records, but also, some of you may be aware of the Green Button Initiative for open energy data access. I've been talking with some colleagues lately about even expanding beyond that to just a general set of recommendations of how we can use all of these building blocks in lots of different areas. We are really on the cutting edge, here, and doing some exciting things with all of these pieces.

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

You said that you came up with the conclusion, in RHEX, that you must use assigned tokens?

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

Yes.

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

Who checks the signature, then, and are there constraints on—well, who checks the signature?

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

It's basically whoever wants to check the signature. It can be either the client that accepts the token from the authorization server, or the protected resource that receives the token from the client. It all depends on how you're actually, you're deploying it, who's going to want to check the signature and how.

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

It would need to be constrained more than that to be really a standard, right?

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

No, not necessarily, because all you really need to define—the important thing to define is how to check the signature so that any interested party that has the token can check the signature. Now, of course, you'll want to specify who has to check the signature.

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

In RHEX, who checks the signature?

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

In RHEX, it was the protected resource.

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

Okay, so that's how it's defined in the RHEX specifications?

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

Yes, exactly—but the way we wrote it in RHEX, the client could also check the signature if it wanted to.

**M**

I think the issue of who needs to check the signature is policy. The fact that a signature is there to be checked is part of the technology specification.

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

Yeah, and the act of checking has to be specified somewhere.

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

Well, yeah.

**M**

It's not always specified.

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

That's available there if you have the policy that you must check it.

**Justin Richer, MS – Lead Technologist – MITRE Corporation**

Yep, exactly, so what we defined in RHEX was, really we actually just, we then pulled something off the shelf there is the JOSE—J-O-S-E—Working Group in the IETF. That's the JSON Object Signing and Encryption, and JSON is itself a Javascript Object notation, so the acronyms just get waist deep very quickly. All that we really said to do was to use what's called a JSON Web Token, which is signed using something called JSON Web Signatures, and we said, "You have a JSON Web Token, it has this stuff in it, these fields in its payload, and it's signed using JSON Web Signatures." Using RSA, I believe we specified RSA 256; it might have been 512 or better, that's what the RHEX profile says. When the protected resource gets handed that token, it can look at it and it knows now how to parse it, because it's a JSON Web Token, so it knows how to pull apart the pieces and do all of the encodings and check all the signatures, and it also knows how to fetch the server's public key using JSON Web Keys.

It can do all of that. We're actually reusing a lot of the same mechanisms in order to build the Blue Button Plus Trusted Registry. We're using JSON Web Tokens, we're using JSON Web Keys and Signatures in order to actually make all of that stuff work. We're gonna see, I think, a lot of the same patterns being applied in different use cases.

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

I spoke to, I hear John, I had asked John—John Moehrke has been working on the IUA specification, and it uses OAuth2, so John, would you like chime in, here? I think I heard you—

**John Moehrke – GE Healthcare**

Sure. Yeah, this is John Moehrke. Yeah, Dixie, the resource server is a very typical place to validate that signature. The format of the signature is well known. The only thing that a standard is going to say is, "What are the trusted identity providers?" That's something the resource server has to know anyway; it has to know which of the token issuers it's going to accept tokens from, anyway, which is administratively an issue, but typically a small issue. I think everything that's been said I totally agree with and incorporated it into the IAG work, so.

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

Dixie, this is David. This might be a good time to get John to do his little presentation, because we're gonna run out of time here.

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

John?

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

Moehrke.

**Male**

And some of us have comments we've been holding.

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

Yeah, that's what I just asked him; to talk about IHE.

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

Okay. That's what I'm—John, I'm encouraging you to not just answer the question, but go forward.

*[Laughter]*

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

Yeah.

### **John Moehrke – GE Healthcare**

I'm sorry. I didn't want to overstep the bounds. Yeah, IHE has also been involved in all of these efforts and a profile proposal was brought to IHE and it was brought by not just IHE itself but also FHIR, also Continua, also DICOM, which is doing RESTful DICOM services, as well as some of the other things that have been talked about.

What IHE did was, they looked at the profile and stuff that RHEX did and said, "Absolutely agree, off the shelf OAuth2 is the appropriate thing to hang our hats on. It is maturing." I think I agree with something Wes said earlier that I think the expectation of maturity is a little over-exaggerated on the previous slides, but it is certainly the place to hang our hats. What IHE looked at is, what's the value? What's missing? Really, IHE says that the piece that's missing is, sometimes the resource server has to make additional access control decisions. Maybe it has a differentiation between roles. Maybe it has a differentiation between purpose of use—treatment versus break glass versus research or what have you. Maybe it has a differentiation between whether it is managing the consents or whether the OAuth authorization is managing consents.

What IHE really focused on was saying, "Yes, we totally buy into the work that RHEX did and incorporated it," but where IHE is really adding value is to say some additional healthcare specific credentials should be carried within that JWT Token which, again, the JSON Web Token, which was just indicated as part of RHEX. That JSON Token is a consumable body within the resource server, and what we wanted to do was, we wanted to make sure that we provided the same kind of deterministic place to put a role that the user is playing or to put the purpose of use that the user is expecting to use the data. Effectively, that's the sum total of the profile is to simply say, "These are attributes that we've learned from the XSD and XCA and XDR environments, where necessary for healthcare, and this is how you would encode them in an OAuth2 using JWT Tokens so that the resource server has the information available if it needs to make additional access control decisions." We left it up to the resource server to say whether it does or doesn't need to make additional access control decisions.

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

John, this is David. That's a great summary, and maybe you're gonna speak to this in a second, but did you not also leave SAML as an alternative to JWT, and could you talk about that if it's appropriate?

### **John Moehrke – GE Healthcare**

Yeah, indeed. The IUA profile also does allow for tiering of a SAML assertion instead of a JWT Token, so it can be a SAML Token. The reason for IHE to do this is twofold. One is, it's real easy, because we've already defined the SAML assertion under the XUA profile and it has met the needs of health information exchanges there. The use cases where one wants to use the full feature set of OAuth to support this authorization that the consumer can do to a particular application, but for which you know your back ends and need a SAML assertion, or for which your identity provider is natively SAML.

You don't have to have an either/or scenario. From a client's perspective, it really doesn't matter what kind of token is requested, but from a resource server perspective, if the resource server needs a SAML assertion, it can get a SAML assertion using the OAuth infrastructure and that way you get kind of the best of both worlds in that if your identity provider is indeed a managed identity provider specifically for healthcare, like maybe if a health information exchange or a regional health information exchange identity provider can be issuing SAML Tokens using the OAuth infrastructure, which gives the end user this ability to say, "I authorize this application, but not this application." It's kind of the best of both.

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

Does—so this is David, again—does pulling in SAML pull in additional complexity that itself needs to be constrained, or is there kind of a working assumption of the right subset of SAML that people just use? My concern of opening that door is just complexity. I certainly understand the logic of how it got there, but are there tradeoffs?

**John Moehrke – GE Healthcare**

Yeah. I think the biggest complexity is, that is probably less mature from an implementation perspective. If you look for off the shelf OAuth providers, they probably are less likely to have the ability to carry a SAML assertion, whereas they're most likely to be able to carry a JWT Token. We actually also indicated that, just because you're doing JWT Tokens in the OAuth conversation does not mean that your resource server can't use WS-Trust to convert an appropriately created OAuth Token into a SAML assertion. You can actually delay that creation of the SAML assertion until the resource server needs it. I think it's more of a maturity question.

**Debbie Bucci – Office of the National Coordinator**

Hello, this is Debbie. I've also often heard that referred to as a SAML bridge, because there are so many off the shelf products that support SAML, and until they can go to the more likely JSON type, it's just that—it's something that you need to be able to have that bridge.

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

You know—thank you, Debbie. Speaking of the maturity, let's go back to Wes and Walter's question. Can you display the maturity slide for everybody? We have a lot of people on this line that really have a deep knowledge of these standards. Let's have them look at that picture and see what they have to say about it. Does anyone—

**F**

What slide is that?

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

Pardon?

**F**

I'm sorry, what slide is that you're looking for?

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

The slide that shows the maturity of the different—let me see if I can bring it up here and see. It's slide 21, the little square, quadrant—four quadrants. While she's doing that, Wes, you started talking—I interrupted you and asked you to hold it, but you had some comments about the maturity of FHIR?

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

Actually, I didn't so much have comments as questions on how we got there, observing that—a couple points. One, just following the list server, lurking on the list server, I find that it's in a stage of very rapid evolution now, which I think is wonderful, but if we think about issuing a spec, at some point that would go into the certification process for Meaningful Use, at that point, FHIR itself has to become reasonably stable and the specs that are written overlying FHIR for the specific use case have to be stable. Early stabilization is not always good for a spontaneous standards effort, so I'm just—I don't have any specific comment. I'm not saying “yea” or “nay” or “whoa” or “go ahead,” I'm just trying to understand where we are.

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

Well—

**Peter N. Kaufman, MD – Driest – Chief Medical Officer and Vice President, Physician IT**

Can I answer the confusion on FHIR a little bit? This is Peter Kaufman. I was on the original work group that wrote the CCR and it was human readable—limited data set, but very standardized, and then that got converted into an HL7 language as the CCD. Then—I know I'm simplifying this—and then that got converted into CDA language as a consolidated CDA. The CCD and the CCVA are not human readable, and now we're seeing FHIR which, again, has the standardized [*Cross talk*].

**M**

I'm actually sorry to hear someone revive the CCR discussion.

**M**

I'm not reviving the CCR, I'm saying, how do you expect the vendors to jump on board with this, when every 18 months there's a new standard that's not compatible with the others.

**M**

I'm sorry—

**Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT**

This is Pete, if I could just make some clarifying comments on what, on some of this discussion since I've been involved in FHIR development?

**M**

Yeah; go ahead, Pete.

**Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT**

There are—FHIR is a collection of resources, and is the specification that has basically a definition for how to produce a RESTful API out of resources. Different parts of the specification are at different levels of stability. The parts of the specification that deal with the resources at a very atomic level dealing with problems, medications, allergies, et cetera are in the process of being developed by the domain committees, and they are actually working off of the initial set of content just based on the Green CDA work, which is based on the CCD work, which is based on the CCR work. They're just simply in the process of developing it. That work is rapidly evolving, as Wes says.

**M**

Would you explain the infrastructure [*Cross talk*].

**Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT**

I'd like to continue, I'd like to continue—just to finish. There are other parts that have to do with infrastructure about how searching is performed, about how the API works, and about some basic endpoints for being able to get at collections of document content that are fairly well stable. I believe the first draft of this, that is expected to go out to ballot, is going out to ballot sometime in the—is going out to something more than just a for comment ballot in the next six months, and that we'd be looking at a BSTU, Brass Standard for Trial Use, which is what many of the specifications that the HIT Standards Committee and ONC have actually identified for use for Meaningful Use in the early part of, I think it's the first half of 2014. It would be available for use, I think, in this context.

I think the statement that it has a moderate level of adoptability, if you were to look at the whole thing, that would not be an accurate statement. If you were to say, "The parts that we need, the parts the Blue Button Plus used in its initial specification are at that level," that would be a more accurate statement. Because in Blue Button Plus, we did not pick the stuff that was rapidly evolving; we picked the stuff that was more or less stable, and so I'll stop there and—Keith, again.

**M**

Could you explain, could you explain—

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

I want to explain—one point I wanted to make about the chart here that we see is that this chart, ONC asked us to make, come up with these metrics not only just to decide yea or nay it's ready to become a standard, but also to recommend to ONC where they put additional resources into either development of the standard or piloting of the standard, et cetera. If this group believes that we should recommend that ONC put more resources into piloting whatever or development, we should say so. That's another purpose of this chart.

**M**

Sorry to keep bugging you on this. I'm trying to understand the need for FHIR. Can somebody explain in English why the CCDA needs to be changed to FHIR? What is missing from CCDA, what is it that makes FHIR a standard that's necessary since it's not yet mature and we have a standard that's someone more mature that healthcare IT companies, vendors, are starting to look into adopting?

## **M**

Let me explain something to you about the Blue Button Plus Pull. The Blue Button Plus Pull enables you to query for a collection of CCDAs and retrieve the CCDAs, so it's not an either/or question about FHIR. It's a question of, "How do we find the documents that we need?" In NwHIN Exchange, you have a query capability to locate documents, but you don't have a RESTful way to query about them or access them. That's what the first phase of Blue Button Plus Pull provides is a RESTful way to query for CCDAs and be able to then download those specific documents that you need. It's not replacing CCDAs for content in this first phase.

There are subsequent phases that will enable access to more granular levels of data so that you can say something, state a question like, "What are the patient's A1c measures for the last two years," for which we don't have a CCDAs document, but we could have a RESTful FHIR query to support that. That is the work that's presently going through rapid revision and innovation, et cetera, and is at not a high level of maturity. That's work that's currently, the working groups in HL7 are spending a lot of time figuring out what the structures of those are. I don't think that's in our discussion at the moment. I think our discussion was the pieces of FHIR that sort of Blue Button Plus is looking at.

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

Yeah, this is David. I'll speak as a representative of a vendor that the CCDAs has evolved into a document standard, even though technically, theoretically, it could be thought of as a messaging standard, but no one is using it that way because of the complexity and the size of a typical CCDAs document. FHIR, on the other hand, gives you a much more granular approach, and it removes a lot of the crust and complexity that has crept into the CCDAs. At least some of the vendors are pretty excited about FHIR as a more efficient, simplified, straightforward way for more granular access in and out of the record and the Blue Button Plus and some of the hData work that could be easily migrated to FHIR in these two profiles that we've looked at are good examples of that.

### **Jitin Asnaani – AthenaHealth**

Hi, this is Jitin—

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

I think we need to—excuse me—you know, we have like one minute, according to my clock. I really don't want us to go down a path outside of our realm, which is security; that's what we're really considering. I wanted to really decide, do we—this meeting is scheduled for an hour and a half. Do we need another meeting to discuss the security issues around Blue Button Plus Pull and—well, the standards that the NwHIN Power Team has recommended? Whether we want to continue the discussion, whether we feel, whether this group feels comfortable in supporting the recommendations—what do we need to do for our next step? The focus, remember, is on security. This is a review by the Privacy and Security Work Group. Walter, why don't you—

### **Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente**

I would say—yeah, thanks, Dixie. I would suggest we schedule another call, because clearly, we've run out of time, here. The next call would really focus on not so much the review of this, but now as the final decisions, if you will, the final consensus and ultimate recommendations that we want to make. That would be my suggestion, that we schedule a new call.

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

Others?

### **Keith Boone – GE Healthcare**

I would agree that more discussion is needed on content. I think, on the security piece, I feel very comfortable with the security—and this is Keith.

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

Dixie, this is David. The only thing, I wonder what the group thinks about some of the questions of the optionalities in the OAuth2 framework. We've debated the JWT, various signing methods, SAML, not SAML—is there a need for more in considering what the right combinations of those choices are, or does the group feel like that's well covered by the work in progress?

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

I'll tell you what let's do. Why don't, David, you, me, and Walter as the chairs of these two groups—why don't we, offline, come up with a list of security specific questions, issues that we think this group should really take on and reschedule a follow-on meeting that specifically addresses those questions?

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

Yeah, I'm happy to do that, and I would say anyone who you didn't name that has thoughts about what those questions ought to be should e-mail us.

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

Absolutely. Anybody on this call, additional security specific questions that you would like for us to discuss at this next meeting, send it to any of us—Walter, myself, or David or all three, doesn't matter—and we'll schedule a follow-on call. I think that's the right answer.

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

Yeah, I agree with that.

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

Okay. Let's open this for public comment, and I want to thank everybody for dialing in. This has been a really nice discussion. We had several people on this call who are new to the NwHIN Power Team, Jitin Asnaani, Keith Boone, and Josh Mandel, and I want to welcome you all to that Power Team, as well. Can we open it up?

**Public Comment**

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

Operator, can you please open the lines?

**Caitlin Collins – Project Coordinator – 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 do not have any comment at this time.

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

Okay. Thank you, Caitlin, for you guys' support and for being responsive to our needs as they evolved, here. We appreciate it. All right, we will be scheduling a follow up call. Any questions, just send them ... thank you all.