



**HIT Standards Committee  
Transport and Security Standards Workgroup  
Final Transcript  
October 8, 2014**

**Presentation**

**Operator**

All lines are bridged with the public.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Thank you. Good afternoon everyone this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of Health IT Standards Committee's Transport and Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Dixie Baker?

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

I'm here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Hi Dixie. Lisa Gallagher?

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Hi Lisa.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Hi.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Aaron Miri?

**Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas**  
Here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Hi Aaron.

**Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas**  
Hello.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Brian Freedman?

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**  
Here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Hi Brian.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**  
Hi.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Jason Taule?

**Jason B. Taule, MS, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems**  
Here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Hi Jason. Jeff Brandt? John Hummel?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**  
Here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Lee Jones? Oh, hi, John, I’m sorry. Lee Jones? Peter Kaufman? Scott Rea? Sharon Terry? And Steven Lane?

**Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health**  
Here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Hi Steven. And from ONC do we have Julie Chua?

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services**

Yes, I'm here.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Hi, Julie.

**Julie Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services**

Hi.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

And with that I'll turn it back to you Dixie and Lisa.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

All right, thank you very and Julie I'm glad you could make it I thought you probably wouldn't be here today. Glad all you could make it, thank you very much for dialing in. Today's meeting is going to be a combination...let me see where are we...we can...oh, this is the agenda, yeah, today is kind of a combination of tying up some loose ends that we left from last meeting when our presentation ran a bit long and we didn't have a whole lot of time to discuss the presentation and we also didn't have an opportunity to discuss the work plan.

So, the first thing we're going to today is to look over the draft work plan, it's at a very high level but you'll get a sense of the kind of topics we'll be addressing in the near future and then Lisa the Trustmark presentation at the last meeting, like I say, it went to the end and we really didn't have time to really sort of pull it into the context of our work plan and what we're trying to do so it wasn't really clear, you know, what do we do with this now that we've heard it and Lisa Gallagher has agreed to present some tools that grew out of the pilot that we heard about the last time and she is going to briefly go over that and she'll provide you with a longer, I think has provided you with a longer presentation that go into more detail.

The main thing in today's agenda is a presentation by Justin Richer who is going to present the Blue Button Plus, Blue Button Plus is the next generation of a Blue Button which are standards to enable individuals to download and send to third-parties, download the EHR and send it to a third-party. And Blue Button Plus uses the OAuth 2 standard which embodies the OpenID Connect and he is going to talk about really all three of those as they relate to consent management in our work plan.

Then we'll have some questions and answers around Justin's presentation, discussion of where we go from here and leave time at the end for public comment. So, are there any questions about what we are going to talk about today?

All right with that let me turn it over...let me go to the next slide and let's review the draft work plan. What you see now is the really high-level work plan for the Federal Advisory Committees and from that, based upon that we go to the...you can really see there that one of the...some of the key...a couple of the key items on the FACA work plan are the strategic plan, the roadmap that's being developed by the ONC, the estimates I think is the NPRM, Meaningful Use NPRM for Stage 3 which should be out toward the end of this year but it is not clear exactly when it will be coming out.

The most immediate event, which is going to be...it's a big event, which is next Wednesday is the first ever joint meeting of the Health Information Technology Policy Committee along with the Health Information Technology Standards Committee and it's an all-day meeting to be held in person in Washington and you will be able to dial in if you're not able to make it, but that should be a very interesting meeting with interesting discussion, and certainly an unprecedented group of people together at a time. Next slide, please.

This is our draft work plan. Right now we're in this period called presentations to inform future work and the future work really is kind of around identity management, consent management, patient identity and some of the presentations that we're looking at now are exactly that, are presentations to inform these future recommendations that we'll be asked to make. The first of these presentations was a Trustmark pilot, we heard at the last meeting, today is Blue Button Plus and OAuth 2.

At the next meeting we'll be hearing about the UMA. UMA is User Managed Access which is a profile of OAuth 2 and that will be presented by Eve Maler who Chairs the UMA Committee. So, that will build very nicely on what you hear today.

Then after the...and then we'll have a presentation about identity management, after that ONC will talk to us about what it says is the rules of the road but it's really the expectations and the needs that ONC has from this group with respect to the interoperability roadmap.

We'll be commenting on the certification NPRM, this will be the 2015 certification criteria and standards, and then finally we'll be commenting on the interoperability roadmap when it is finally published and the latest thing, the last thing we'll be addressing is data provenance. Okay, from that are there any questions about what we have in front of us?

Okay, Lisa would you like to move ahead and talk about the tools that grew out of the Trustmark pilot that we heard about at the last meeting?

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Okay, thank you, Dixie. If you could go to the next slide of my presentation, okay, the next slide, I had...there we go, okay. So, I wanted to note that first of all I have extracted these slides from various presentations, they're available on the public website of GTRI relating to this pilot and so I say here that, you know, they're the source of these slides with permission. Next slide, please.

So, coming out of the last meeting Dixie and I chatted a bit and one of the things that I think we didn't cover in a lot of detail was the fact that aside from doing an actual pilot with trust criteria from, you know, various sort of federal programs GTRI has also created an infrastructure for the development and promulgation of Trustmarks by various stakeholders and they actually have quite a robust toolkit, they have some standards, and they also have some sample documents so I just wanted to go through the part of the pilot that is that set of tools.

Just as a reminder on this first slide I think one of the things that impressed me most about their approach is the concept that we could take trust criteria from various sources and analyze and distill them into modules or components. So the componentization of trust was a particularly intriguing point for me. The benefits here of that approach are of course, you know, within each trust framework the requirements tend to be opaque and this could bring transparency to those requirements, ease of comparability between the requirements of different frameworks and the possibility or potential for reusability of those components. They call the modular components of trust Trustmarks. Next slide, please.

So, then, you know, as we look at different trust frameworks it is important to note that the trust requirements could be expressed again in terms of a modular set of components and the set of those components could be described for each trust framework as a trust interoperability profile and I think that's nicely depicted here. Next slide, please.

And so then there could be many Trustmark providers in an identity ecosystem and Trustmarks can be acquired through a Trustmark provider and each member of the community can acquire the necessary Trustmarks based on the Trustmark profile for their trust framework. Next slide, please.

Let me make sure I'm...and next slide, okay, this was a layered slide, so next slide, please. Okay. And then Trustmarks that are created by various stakeholder groups could be stored in a Trustmark registry that is searchable and could be shared among partners as well. And next slide, please.

So, I extracted this slide from John's presentation from last month, last meeting and it's important to note that as part of the pilot work they have provided some tools and sample documents and I have circled those in red here on the slide.

So, there are two categories of tools, there are some tools that allow folks to create Trustmarks so various stakeholder groups can create Trustmarks and we'll go over the process for doing that. There is a repository, there is actually a Trustmark assessment tool, Trustmark generating and publishing tool, a query tool and then some sample documents as well as a standard for describing a Trustmark. So, that's part of the pilot. While they are actually using this framework to distill some various federal requirements they have developed the structure for the whole entire ecosystem. Okay, next slide, please.

So, how would we or anyone as a stakeholder group go about developing Trustmarks that work for them? Next slide, please.

So, here is a slide that talks about the Trustmark framework and the process for developing a Trustmark. So, you start with a stakeholder community that has a certain need, so it could be a government agency with, you know, a set of federal requirements or it could be a community of interest, a sector, a private company, etcetera. They are then represented by a Trustmark defining organization, so they take the needs of that stakeholder community and it could be representatives of the stakeholder community itself and they document what are the requirements. Those requirements are then translated into a Trustmark definition and there is actually some structure for that that's provided in the GTRI toolkit as well and we'll cover that.

Then there are those who want to receive a Trustmark, there are those who issue Trustmarks, so Trustmark providers and then there are those finally who rely on the Trustmark for entering into transactions so those Trustmark relying parties and that's sort of, you know, how the process is framed. Next slide, please.

So, again, as John stressed there are many sources of trust components. Here for the GTRI pilot those are largely from federal programs and other government related programs but it's important to note that the generic process does facilitate the implementation of trust and interoperability components from other sources, any other source. Next slide, please.

So, at the highest level the process looks like this, the trust and interoperability requirements can be gathered from multiple frameworks, single framework or multiple frameworks whatever is relevant to that stakeholder group and then those requirements can be broken down and re-assembled into modular reusable components. And these modularized components are then expressed in a standard format in order to encourage broad use and this results in a set of Trustmarks and each Trustmark has its associated Trustmark definition. Next slide, please.

So, here we have an example of...I'm sorry, next slide, next slide, next slide, okay, sorry you guys didn't get to see this while I was describing it, okay, so you gather the trust requirements and the interoperability requirements, you break down and reassemble into modular reusable components and then express those in terms of Trustmarks in a standard way to encourage reuse and that takes the form of a Trustmark definition. Okay, next slide, please.

So, here, you know, this is a busy chart, but really what it is, is a chart that shows how GTRI took the various requirement sets that I showed on an earlier slide and distilled them into modular components of trust or interoperability and they've catalogued them. So, they cover a specific set of federal requirements, they also cover FIPPS and it ended up that they had identified 122 distinct Trustmarks or components of trust resulting from this pilot. Next slide, please.

But, I think even more important is this slide, while we might not use or come up with a set of Trustmarks that look like the ones that GTRI developed with the federal requirements they have categorized those Trustmarks that they developed into categories. So one can see that these categories are intuitive and they are largely applicable to the health sector.

So, because, you know, the ones that they developed may not be usable by us the categories are probably applicable to healthcare data exchange and Trustmarks could be developed to meet those needs, but my guess is that the categories here are broadly applicable and would even provide guidance in the development of applicable Trustmarks should we decide that we wanted to do that. So, I'm not sure if John had this slide in his slide deck last time but I did find it on the GTRI website, so you can see that they've defined these broad categories and they've mapped each of their defined Trustmarks to those categories. Next slide, please.

This is just a slide that shows the proposed standardized Trustmark component definition specification document. So, what it does is it provides a format for a formalized articulation of the requirements and it describes the components of that in a well-defined format includes things like unique name, definition, conformance criteria, conformance target, version, citations, assessment process, various components and this allows folks to understand the requirements but also does that in a standardized way via this Trustmark component definition specification. Next slide, please.

And so finally on the last slide it just shows that there is a notional process in place for evaluation of proposed Trustmarks, you know, specified in the form of Trustmark definition documents and those can be submitted for review, for conformance to the standard and can also be housed in the repository for search and reuse.

So, that's just a quick rundown of the tools that are available in the GTRI toolkit. There is also a sample document for almost everything that I've gone over and so with that I'll throw it back to you Dixie but I just wanted to, you know, cover the part that I think is more generically applicable to various stakeholders and make sure that everyone was aware that those tools are available and entertain any questions. I'm not an expert on this but I did look through it pretty thoroughly.

**Steven Lane, MD, MPH, FFAFP – EHR Ambulatory Physician Director – Sutter Health**

This is Steven Lane I'll just comment that I think that summary was incredibly helpful; it certainly helped to solidify my understanding of the topic.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Well, thank you.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Well, I still...I find it very confusing myself because, you know, on the first...I guess it was the second slide it says that the modular components are Trustmarks and so I'm going, you know, light bulb "oh, okay" so these components themselves are the Trustmarks and then as we move on slide 10 shows this funnel that shows a Trustmark definition as being something produced from the components which...

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Right.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

On slide two said were the Trustmarks.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Okay, so if you go to slide...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

I find it, I find it very confusing myself.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

If you look at slide two I think it is a little misleading, the blue boxes that have FICAM and FIPPS those are the sources of the requirements that are modularized and put into those Trustmarks that are represented by the shapes. So that is kind of misleading.

So, basically you take a whole bunch of requirements and you look at the common elements that sort of try to componentize modularize them and define those as Trustmarks. When you look at the categories than you would see, you know, there are several privacy related, you know, Trustmarks and security related Trustmarks and elements of, you know, agreements such as identity assurance, I mean, technical trust and other things like usability. So, you're taking what's a set of various requirements and sort of distilling them into groups and creating Trustmarks from those groups. Does that make sense?

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

And then you create a profile that then selects components from the, you know, you've got a Trustmark that has a whole bunch of privacy statements let's say, right?

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Right.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Then what do you do? You select the ones you want to use?

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Yeah and then everyone else outside of your trust framework would know which Trustmarks you used and would be able to understand what those are and that's where you can then communicate elements of trust across trust framework.

So you're really taking requirements and filling them into a common language and common format and common sort of intuitive modular approaches so that there is transparency and there is ease of comparability, and those sorts of things and also reusability so when you have a new trust framework you can use components that are common and known to others.

**Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas**

So, basically, this is Aaron from Children's, so basically I'm thinking of this from an analogy perspective, this is like a driver's license and what you're doing is you have standard elements of a driver's license your name, you know, your address those kinds of things but if you're a donor or not, or what state you're in or whatever else those are elements that we'll pick and choose and put on it so it's just like a trading card basically.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Right and it also allows you to understand what another state does because you're selecting from a common set of marks.

**Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas**

Yes, that makes sense, okay.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah, yeah, yeah.

**M**

So...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

How do you assure that there is a common level of assurance or is there a way?

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Well I think if you look at slide 12 where it suggests some intuitive categories and that's where you would work on this. So, we would work on the elements that are important to us as far as cross, you know, cross HIE or cross networks trust, you know, so those would may be unique to healthcare data exchange, you know, you would define those and create them as needed.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

I see.

**Jason B. Taule, MS, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems**

So, Lisa and Dixie, this is Jason Taule, how are you?

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Hi.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Great.

**Jason B. Taule, MS, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems**

I want to...this is the first presentation that I've sat through and I want to compliment you guys number one on getting the modular component right and emphasize this as something that was missing in prior attempts to solve this challenge. It is not one simple use case that we have out there that we need to support with these questions that we need to solve. And if you don't have a modular solution you don't allow different business owners with different kinds of information and different kinds of systems, and different user populations to make different determinations about what level of trust and assurance they require to get a level of comfort to allow people to exchange information.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Right.

**Jason B. Taule, MS, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems**

Only by doing it through a modular approach can we achieve that in a way that then the infrastructure is reusable and the cost burden is spread across many different systems as opposed to be borne by one.

And then the second question is one that I think is well downstream, the one that Dixie was just asking, is once we establish all these Trustmarks and we figure out different ways to put them together to give people that level of confidence then the question is how do we trust the Trustmark.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah.

**Jason B. Taule, MS, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems**

And I think we can borrow from other areas where we've established security, you know, whether it be a certificate or a private key that is stored in a registry and there are mechanisms for doing that.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Yes and that would be something we would look at as a sector as well.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah, I have to observe that this is quite similar to the common criteria.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Yeah, I think there are some...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

...evaluation that's kind of how you do it, exactly.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Yeah, yeah. So, Dixie, time check, I know we need to move on.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yes.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

I just wanted to make sure people are aware of these tools.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yes, I really appreciate you going over it and I think that your description today really did help us understand the relevance of what we heard at the last meeting, so thank you very much.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Thank you all.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Okay, back to our agenda, I believe the next thing is our presentation from Justin. And I want to thank Justin for coming I know he's actually on sabbatical from MITRE right now but we especially requested that he do this for us because I've heard him talk about Blue Button Plus before and he does such a good job so thank you very much Justin we appreciate it.

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

Well, thank you for inviting me and I'm actually back from sabbatical now.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Oh, okay.

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

So, yeah, back to the day job, the sabbatical was definitely fun though.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Good, good.

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

So, shall I just dive right in?

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yes, yes.

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

All right, so first thank you to Dixie and everybody for asking me to come along today. The way that I've written this presentation is that I've tried to keep things at a relatively high-level but I am more than willing to dive very, very deep into these things as much as I'm able to and so I welcome questions as we go along and so let's get started. Next slide, please.

Some of the background here is that the original Blue Button was designed around patient right of access to healthcare data. The idea was to have a simple Blue Button, I believe the phrase was "a dam Blue Button" on the page that allows the patient to just click and download a copy of their record in whatever format it was, and this was good in that it allowed access to the data but it was...it stopped a few steps short of making the data particularly useful or specifically reusable by the patient.

So, what you got was usually fronted by a portal where you had to log in and do some human interaction to go and click the Blue Button and it could have been a text file, it could have been a PDF, it could have been an XML file, there are a lot of things that could have shown up after you clicked on the Blue Button. There were some common files but nothing really saying exactly what had to be in there. And these were generally one-off reports. So, you clicked the Blue Button you get a snapshot of what's there and then that's it, if you want an update you have to go in and click the Blue Button again. Next slide, please.

Which brings us to Blue Button Plus and the idea here is to move beyond download my data into the world of connect my data and we really wanted to provide a machine addressable API to that data so that you could actually move the EHR from one machine to another in a way that it could actually be parsed and understood and incorporated, and eventually connected in multiple directions to multiple providers all at the behest of the patient themselves.

There are two transport and access mechanisms that were developed in the Blue Button Plus umbrella the first of these is the Direct Project which I know many of you are familiar with that uses S/MIME or encrypted e-mail and you can think of Direct really as a modern replacement for the fax machine because you're really still sending a record kind of from one side to another and in many cases it is structured and you can ingest it but there is not really a whole lot of API going there because it's e-mail and there is not so much you can do with that.

The other major mechanism under the Blue Button Plus umbrella is the RESTful protocol and so that's what I'm going to talk about today. But for both of these it was very, very important that there be common security models so that the software and application developers that are going to be requesting this data programmatically or sending it across the wire or ingesting it they know what to expect, they know how to get a user's right of access conveyed to the far side and how to ensure that the right people get the right data and it doesn't go leaking all over the Internet because I think we can all agree that would be bad. Next slide, please.

So, specifically the Blue Button REST API set out to profile a handful of different technologies and bring them together under one profile definition. The first of these is of course FHIR, which I always forget what it stands for it's like Fast Health Interoperable Resources, it's a beautifully convoluted acronym, but we picked a small subset of FHIR as it was available at the time, and this was January 2013 that the Blue Button Plus work really started to kick off, and we settled on OAuth 2 for access delegation.

And I'll get into a little bit about what exactly OAuth 2 does and how it works in a little bit, but suffice it to say that OAuth 2 at its core allows a resource owner, an authenticated party to delegate some subset of their right of access, some subset of their authorization to a software client and this very well fits the Blue Button Plus goal of allowing a patient to give an application access to their healthcare record over a programmatic API.

We augmented what was existing in the standards of OAuth 2 and FHIR with a couple of other components that kind of help build up the trust model and really build up the application ecosystem. So, if you read through the Blue Button Plus REST spec you'll see there is mention of a registry component which provides discovery and a form of a trust anchor, this is not the same as a Direct trust bundle but they're analogous in some interestingly fuzzy ways and we came up with a way to have a...using OAuth dynamic client registration to have different levels of clients application within the system based on what the client is capable of.

As we just heard in the trust framework presentation not everything is going to be kind of a one size fits all solution, in fact we know that it's not going to fit all. So, in Blue Button we actually defined six different distinct classes of client application that were totally valid within the Blue Button Plus ecosystem but would all have to be treated a little bit differently.

So, you've got for example a JavaScript client sitting in a web-browser you're going to treat that very differently from a native application running on somebody's smart phone, you're going to treat that differently from a web application that is sitting on a trusted server that is run by an insurance company or other vetted organization. All of these have different profiles and all of them have different aspects that you care about when you're going through this.

So, even though in all of the Blue Button cases it is the patient who is making that trust conveyance decision we wanted to be able to inform the patient appropriately with what rights they were really giving up, not giving up I should say, what authorizations they were allowing I should say, not giving up rights, sorry, and what they could expect out of different classes of clients.

And we wanted to give developers very clear guidelines of what part of the profile applied to them. So you could look at the code that you're writing and I'm going at this as a software engineer and architect, look at the code that you're writing and say, oh, well I'm doing something that looks like this and something that looks like this, oh, I fit into this table cell, you know, this describes me, this tells me exactly what I'm doing, because by making it very easy and very deterministic for developers we're hoping to actually gain a lot of traction in the development community. Because at the end of the day standards are kind of a dime a dozen and they're not really standards unless somebody is actually implementing them.

So, we added some components with the registry and the trusted registration to facilitate those different classes of clients and some more in a bit about where those went because that's kind of an interesting story and I'll try to spare you all the details.

Next up we worked on a set of standardized OAuth scopes, now a scope in OAuth is a way to programmatically limit access to a particular resource and particular client in its context. And OAuth doesn't define the scopes themselves or what they apply to because OAuth could be applied to any API, RESTful or not as it turns out, on the web. Any web API can pretty easily be OAuth 2 protected but we knew the API, we knew that it was a subset of FHIR so we defined a set of scopes and we actually structured those so that they would work with the Blue Button use cases and the bits of the FHIR API that we were working with.

And finally, next slide, please, we developed the entire thing in the open on GitHub so if you Google for Blue Button Plus REST API you will eventually come across our GitHub repository and the core developers of this specification, this profile we tried to do all of our work as much in the open as possible. We think that is absolutely vital for standards definition and for capturing the kinds of concerns that different stakeholders from the clients to the resource providers to, you know, authorization providers and whatnot would actually have in the standards itself and we found that to be a very effective means of collaboration. Next slide, please.

So, Blue Button Plus I'm a little sad to report today that it's kind of stale at the moment. Since the initial definition of Blue Button Plus there have been a few efforts to kind of get pilots up and running and get people on board but there have not, to date, been any successful bilateral pilots which means that there have been some interesting demos and lots of interest from the application developer community, the people who want to consume the Blue Button Plus API they really, really, really want this, but there hasn't really been engagement from the EHR provider community.

The EHR vendors and folks, and organizations, and folks of that ilk don't seem to want to enable this type of dynamic run time, patient-driven access to the system. Because of that, because we haven't really had a lot of push behind getting it actually up and running the technology definitions themselves have gone a little bit wonky.

As it turns out FHIR is in continuous development, there have been lots more stuff that has been added to it so the definition that we have in Blue Button Plus doesn't exactly match what is there in FHIR today, it could be aligned pretty easily but nobody has really asked to do that right now. Again, owing to the lack of on the ground pilots.

There have also been some interesting things on the security standard side, that Blue Button Plus registry and kind of the trusted client registration that I had mentioned before, many of those components have actually been adopted into the IETF draft standard of OAuth dynamic client registration, caveat emptor I am the editor of that spec so I'm a little biased to say that we made the right choice in bringing those in.

But, in any case it's done in a slightly different way from what Blue Button Plus defined at the time which one would expect because Blue Button was defining it in the scope of Blue Button whereas the IETF spec has to define it in the scope of all OAuth applications. So, it's a little bit different but the spirit is really there and Blue Button could very easily be aligned with that, but again, no call for that yet.

There are some other aspects like this that could be factored out of Blue Button Plus the scope definitions are really kind of a key big one, but one of the biggest ways that it's kind of gone in a different direction is that at the time Blue Button Plus REST was focused on fieldable Meaningful Use 2 compliant things, which is getting a particular kind of XML file out of the end-point when the user asks for it and so that's how Blue Button Plus was written.

FHIR has since gone on to define more discrete and structured data and different security markings and other types of resources and end-points that you can add into this that Blue Button Plus really should be using, but that hasn't been incorporated yet. So, that in a nutshell is Blue Button Plus.

I'm going to pause and take a breath for a moment. If anybody has any questions on this part before I move into some of the underlying technologies and protocols? Unless of course you'd like me to just go through to the end and take a stack of questions at the end?

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

Hey, Justin?

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

Yes?

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

This is Jeff Brandt, first a great job I've been following Blue Button since its inception and to see what you guys are doing and finally getting it to an open API just makes more sense than I could even state, but the biggest problem that I see and as our team...and I'm just going to maybe put this out to Lisa or some of the other people is it's always the same problem, the technology is there, this is easy. What is difficult is getting EHRs to open the doors.

So, I just wondered how would...because, you know, ONC wants to make interoperability but it's not ever going to happen until we put pressure somehow or convince the EHR vendors to participate and one of the things is that we can do...and I know everybody is not going to like this, but if we can figure out a way maybe to monetize the data and maybe that includes the patient as the beneficiary and maybe we can work like all other APIs do across the world is they're monetizing and that's how they become successful just like Facebook. But, thanks, I appreciate it.

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

Thanks, those are really great comments and I've long held the opinion that for instances like this where you have kind of a big ensconced player just kind of sitting there and not wanting to budge. The pressure really needs to come from multiple directions. In this case there are two main ones that I think could be made to exist. The first is kind of the regulatory pressure, the government saying "thou shalt provide FHIR with the following definitions and thou shalt provide OAuth protection to thine FHIR with the following conditions." And that's only one direction though and we've kind of seen how well that compliance really...how far that level of compliance can really get folks.

The other direction and it's arguably equally as important is market pressure. There needs to be sort of application demand for this and we have yet to see, you know, the App developers want to be able to write to this stuff but it doesn't exist yet so they haven't so we're kind of in this weird chicken and egg problem.

**Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas**

Let me ask a question this is Aaron Miri at Children's Medical Center, so I can appreciate your comments and I can appreciate even the tons of frustration at the lack of adoption and I agree with the need for a WIIFM, What's In It For Me, aspect of this whole thing.

I do tend to agree from the provider perspective on the carrot necessary to allow for organizations to consider this or even for EMR vendors to consider this but I would say let's go at it from a different direction.

Right now if you encrypt every single device you have and you lose that device, let's say you encrypted a laptop, you lose the device you have a safe harbor and it was granted trying to push organizations towards life scale adoption of encryption, well guess what it worked. Now most organizations are doing that and if they're not they're going to end up on the news at some point when something gets lost and they are fined millions of dollars we're seeing that over and over again so the adoption rate is there.

Can we get consideration for a set of standards and in this case Blue Button Plus for consideration for safe harbor which would then again be that carrot but not necessarily from a money perspective but a carrot of, okay, look you're doing best practice, you're doing what we consider so therefore you're trying to be a thought leader and do the right thing here, therefore, you know, if something does happen, something is intercepted it's not negligent.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

That's a great comment Aaron. I personally think that one of the problems is that the 2014 edition in the view, download and transmit allows the EHR vendor to implement it as either a human readable downloadable document or a structured C-CDA and in my experience working with a lot of people who are trying to get data for research primarily almost all provider organizations are just doing it, taking...are downloading the human readable and a lot of EHR vendors in fact don't even realize that they have the option to implement the C-CDA structured document it's one of those, "or's" that still exist in the standards and that could be one of the barriers.

But I really like the idea of the safe harbor because I suspect they are a main...allowing a mobile App to, you know, pull data from the EHR is likely to be scary from a compliance perspective right now that's a really good observation I think.

**M**

I think...

**M**

Hey, Dixie?

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

And I just wanted to say that we have seen similar things in the financial industry for pushing compliance to particular technology standards. The chip and pin card rollout that's happening in the United States over the next couple of years is a really good example of that. It's not a one-to-one comparison but I think there is definitely a lot that can be learned in that and I think that's a great idea.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah.

**Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas**

Especially when other countries already put the EHR data, type data, health record data on the chip that's on the card. So, it's yet another.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah, yeah.

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

Yes.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

So you have other slides about the technology?

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

Yes, so, next slide please.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Okay.

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

I will just roll through these.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah.

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

And so now I'm going to talk for a few minutes about some of the underlying and related protocols this really should have been, this slide should have been labeled. Next slide, please. And the chief of these is OAuth 2. I mentioned at the beginning that OAuth is a delegation protocol. Now OAuth often gets termed an authorization protocol that's ostensibly what the "auth" in OAuth stands for. Some people use it as an authentication protocol they're wrong, and I'll tell you why in a moment, but fundamentally OAuth is a delegation protocol.

And you have several parties that work together here to actually transmit data in a secure fashion across the network. You've got a resource owner, there is somebody who has a certain set of rights to access a particular API and I'm going to generally say to get data but it could be to publish data, it could be to do any number of things that the API allows you to do and it's just generic access to a set of verbs on an HTTP web resource.

Now they have a client application that they want to act on their behalf to this protected resource and the way that these are all tied together is through a component called an authorization server and a protocol called OAuth which allows these different things to talk sharing minimal amounts of information in order to make sure that the trust is actually conveyed in an appropriate fashion especially when the authorization server client and protected resource could all live in different security domains entirely.

This is an open standard hosted by the IETF with the two core RFC numbers on the slide there, but importantly this means that anybody at all can implement and use this without charging any or without paying any fees or any licensing or any pattern encumbrance or anything like that. It is widely and freely available and this is one of the several things about the protocol that has led to its wide, wide spread success, hundreds of thousands of APIs and as more come on line every day we're seeing them use OAuth for their protection mechanisms, very, very popular protocol. So, next slide, please.

I'm going to use this diagram to talk through kind of how the different pieces communicate with each other. So, over on the left-hand side we've got the resource owner and they're sitting behind the user agent web-browser generally speaking. They're going to be interacting with a client application. Now this client application could be something native running on a device like a desktop or a phone, or something like that, it could be something running on a web server that they are using their web-browser to access or it could be something running inside the browser itself kind of an embedded JavaScript mobile code kind of client, or it could be something that we haven't thought of yet that can still speak HTTP.

Regardless, the resource owner shows up at the client and the client tells the resource owner I need access to something that you can give me access to so I'm going to send you over to the authorization server to get that for me. And the way the client does this is it uses that user agent, the web-browser, and sends the resource owner over to a special page on the authorization server where the resource owner can approve the client.

Now several things are actually happening here, first since this request is going out through the web-browser the client doesn't have access to anything that goes across that. Second, and that's one way that OAuth sort of limits the amount of information that's known here. Second, the resource owner is going to be authenticating to the authorization server somehow. They're going to have to log in somehow in order to be allowed to authorize a client.

The way that the resource owner authenticates is actually out of scope for OAuth which makes it very, very flexible into the types of environments that you can actually play with. And finally, the resource owner, depending on how the authorization server is implemented, the resource owner could actually be given the chance to give the client less access than they even asked for and the client can, again of course, ask for limited access to begin with because it's all ultimately up to the resource owner and the authorization server what access the client gets.

So, gone are the days where you have a developer key attached to a client and the client shows up to the protected resource with that developer key and it says, here's my developer key which grants me access to absolutely everything and anything on here but I'm going to pretend that I'm acting on behalf of a particular user, so just give me that record for today. Where really that client could be accessing it on behalf of anybody. He could be accessing it on behalf of a bad actor if it's been cracked or whatnot.

What OAuth does though is it gives us a context whereby the client is making a request in the context of the resource owner being authenticated and making an explicit or often explicit I should say authorization delegation decision and you guys have all seen this if you've ever logged into a site with Facebook or connected an application and gotten that screen up that says, you know, the following application would like access to your e-mail address, your name all of that kind of stuff, you know, to be able to post to your web page whatnot that's all OAuth and that is an OAuth authorization screen that you're actually seeing there.

So, the next part is that the authorization server communicates back again through the web-browser to the client something that tells the client a user said you have access now that's called an authorization grant usually expressed in an authorization code there are different forms of OAuth but we'll not get into those particular weeds right now.

The client then presents that authorization grant back to the authorization server directly now here this is the orange line in the middle, it's talking to the token end-point as opposed to the authorization end-point and it presents that code back to the authorization server outside of the browser now at this point the resource owner is not present and not authenticated on this channel. The client, however, is authenticated on this channel and so the client can prove who it is and it can prove that it has a particular access code.

So, the authorization server that minted that access code can say, oh, yeah, this is the same client that requested it and I know the user that said that this was okay. Additionally, I know what the user said it was okay for and how long it was good for and all of that other type of security decision information that you would want gets fed into a token, an OAuth token which is then returned to the client and it is that token, that final artifact that the client presents to the protected resource in order to actually access the API or get the data. Next slide, please.

OpenID Connect is an authentication and identity protocol that is built on top of the OAuth authorization and delegation protocol. It is another open standard in use by a bunch of folks and the key interesting thing here is that the OpenID Connect standard works by saying that the thing that you are delegating access to is your identity information as a user.

So, if I'm going to your site and you want to be able to log me in with my OpenID identity provider I can grant you access to my identity and my session information with that identity provider using OAuth and a standard protocol that's being protected by OAuth and with that information you now know who I am and can prove that in a trustable fashion.

That is effectively all OpenID Connect really is, it's an identity protocol protected by OAuth. What this gives you though is single-sign on that works in a distributed fashion at Internet scale. Now it's important to point out here that the technology works at Internet scale but that doesn't necessarily mean that the trust and policy are set up to run at Internet scale because as I think everyone on this call very well knows those are two very different questions.

But because it allows end-users to carry their identities across multiple different sites it is key in solving the multiple portals problem where you have one patient that needs to go to multiple different doctors, they need to be able...they should be able to tie their identity to different medical records and different access points at all of these different portals.

And also you'll recall that in an OAuth authorization server the user needs to authenticate to the authorization server that is protecting the medical records, right, well it turns out you can actually use OpenID Connect to protect an OpenID Connect identity provider to protect the authentication, the user authentication to an OAuth authorization server and it chains very nicely because they were designed to work together in that way.

And OpenID Connect is fundamental to several NIST initiatives and it's a newer technology it was only standardized as a final standard this past February but it's really starting to gain momentum especially in kind of the trusted enterprise identity space. I think we're seeing a lot of really interesting stuff.

Also, if you've signed in with anything with Google in the last 12 months or so you have actually been using OpenID Connect and you might not have actually known it because Google really likes to brand it. Next slide, please.

UMA, User Managed Access, is something you're going to get to hear a whole lot more about from somebody way smarter than me two weeks from now when Eve Maler comes to present on it, but suffice it to say that it is an application that is built on top of OAuth 2 and OpenID Connect it's a draft, again open standard, no licensing requirements for any of these standards and I really do believe that is vital in their success.

And what UMA really allows you to do is instead of a single user delegating access to a client working on their behalf you can delegate access in a couple of different ways to different users and different applications who can prove themselves using different sets of claims. So, it's a more flexible, more distributed model than standard OAuth but under the hood it uses all regular OAuth constructs and concepts and in fact many of the components that were originally developed in UMA have since been pulled out and re-used and sort of adapted and generalized by other protocols.

I mentioned the OAuth dynamic client registration that was initially developed in User Managed Access whereby a client might show up to an authorization server that it has never talked to before and it therefore needs that client ID, it needs all sorts of other things from that authorization server in order to do the OAuth transaction.

In a normal OAuth world people were kind of ignoring that use case, in the UMA space they were saying, no this is the real thing we need to solve it. They came up with the concept and the original encoding of dynamic client registration and that was then adopted by OpenID Connect, which again being a distributed identity protocol has that same problem of needing to introduce clients to the identity providers. Those have since been merged and are being shepherded through the IETF standards body, the Internet Engineering Task Force, by the way in case I'm dropping unfamiliar acronyms.

They're being shepherded through the IETF standards body as a general purpose protocol for registering OAuth clients to authorization servers. But again more on that in much greater detail in a couple of weeks from Eve Maler, but it's definitely very good stuff and I've been really excited to see, especially in the last year, it really starting to take off and get applied in places. Next slide, please.

The NWHIN group from ONC, which many of you were members of, put out a set of recommendations last summer that talk about how to properly use the building blocks of digital health and focusing on some common core components OAuth 2 for your authorization and delegation, OpenID Connect for authentication and identity federation and FHIR for your data access and your formats and your URLs and APIs and fitting them together in ways that actually solve specific applications.

One that I was involved with a couple of year ago was the RHEX Project, R-H-E-X, which really focused on provider to provider sharing. So we were using OAuth and OpenID but they weren't patients that were delegating access it was a doctor delegating access from one record to another doctor at a different provider site but we were using all of the same building blocks as Blue Button Plus which was focusing on provider to patient access. So, the patient having a certain set of rights to the information can use all of these same pieces to be able to get at stuff.

And the NWHIN recommendation, which I wholeheartedly agree with, is that by using these common building blocks and starting to abstract common recipes from these we can really start to build a health applications ecosystem that is not a single monolithic, you know, build your entire application this one-way to suit all use cases, but instead it's a modular and flexible approach that lets you bring pieces together in ways that actually make sense for what you're trying to do. Next slide, please.

I was told I should talk specifically about how all of this stuff relates to consent management which is kind of the core topic of this working group as I understand. Next slide, please. And I'll start by saying that we've inherited kind of a nasty legacy of consent management from the paper system. So, if you look at the text of HIPAA it says "the request for information must be presented in writing and signed" that's kind of hard to do when it's a smart phone application and we get into very dangerous things by saying like "oh, we have this thing called digital signatures that must mean exactly the same as the physical signature of the patient that we saw before. So, if I digitally sign my request I'm fulfilling all of the letter of the law." Next slide, please.

The problem is that the spirit of the law is, I would argue, rather different. What you're looking at for a consent decision is there is a conscious action, there is a decision point that's made where somebody is either making the specific decision to allow access to a particular set of information or in the aberrant case they are making a specific decision to commit fraud.

So, think of what it takes to forge somebody's signature you have to put the effort into trying to forge that signature as opposed to with digital signatures where you just have to have a copy of certain of bits that represents their private key.

This conscientious action needs to happen in a particular context and it has to take some amount of effort and reliably take some amount of intent. That's the idea here is that it doesn't just happen automatically because certain sets of bits were in the right place.

Secondly, when you have a signature and a consent decision in the paper system one of the key things about that is the receipt, is the verifiable audit trail that somebody stood somewhere and filed a piece of paper with ink on it that squiggle of ink looks right when we look at it later down the line and said "no" but really "it looks like you signed this, did you actually sign this" and like "no somebody forged that." I mean you can start to actually have that conversation around that because there is this verifiable audit trail that's available after the fact.

In many digital systems we have the capability of having an audit trail but because the systems are so distributed and so disjointed we end up losing that in a lot of spaces because my data might be pulled down to an App and sent somewhere else and go somewhere, so where is my decision actually recorded, when was I ever even asked by the system what I want to do. So, we want to be able to store that kind of stuff. Next slide, please.

My argument is that the OAuth authorization process actually gives us a very clear hook into that because there is that explicit decision point where the resource owner is present and authenticated and maybe presented with a set of information that says, you know, hey, such and such application is asking right now to access your stuff and furthermore this is the part of your stuff that they actually want. They want these parts of your record. They want your mental health in addition to your demographics and everything else like that.

This context of the decision being made lets us have both that intent and effort, the user has to be authenticated, they have to be presented with the information and click through that and there is lots of usability research that's being done with this right now, but we can also store the results of that decision. So, the authorization server is actually in a really good place to provide tracking and audit over time.

So, my question to this community really kind of at large is, why are we not considering an OAuth authorization to be a record or consent?

Now, I'll go on further to say that when you hear more about the UMA protocol in a couple of weeks you'll see that there are other kinds of consents that can also be stored and propagated across the network beyond the run time what likes to be called Alice to Alice sharing of, you know, I get to have an application act on my behalf, UMA allows you to express other things like, my data can be used by anybody in the US Oncological Society for cancer research as long as it's anonymized. I can set up policies to allow things like that and express those using UMA, XACML and other things. Next slide, please.

And this is my last point is that there is an emerging standard around consent and notice. So, if you go to [opennotice.org](http://opennotice.org) there is some really good work that's being done here. What we're seeing on the side here is called a consent receipt and the idea here is to have a standardized marking for these consent decisions. This goes, I think, part and parcel with the standardized markings and the machine readable versions of the Trustmarks that we heard about earlier on this call. I think that's really great work that's being done there. And I think that these two could really go hand-and-hand with each other.

And if this API, which is still very, very much in its early stages of development, but if this consent notice and notice receipt API could be made queriable and aggregatable then all of the different authorization servers that I might have to interact with as a person I could actually get a record of not only what data is out there, because I have access to it, but what consent I have left stored at all of these different places, what decisions have been made based on that consent that I gave, because I should have the right to access all of that.

And finally, next slide, that's all I had. Thank you very much. My e-mail address is on the slide if any of you would like to yell at me after the call its right there and I will now finish with any questions or Dixie however you would like to take this.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Thank you for...thank you, we really appreciate that. As usual you're really good as describing things in a way that's very easy to understand and I really appreciate it. I just wanted to...I hesitate to...the comment you made at the end where why couldn't a...authorization be a consent and the audit trail of accesses be kept...just FYI that has been done one of my principle clients does exactly that in their privacy management technology, they use the...you know, they use the OAuth 2 to get the consent and store the consent and then they keep an audit trail, and they've implemented UMA, so that is being done by some people and that technology is used primarily in the research community but that's exactly what they're doing. So, what you suggest is certainly doable and is being accepted at least in the research community.

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

That's really great to hear and I'll say that I have seen instances of this but they all tend to be very kind of limited domain. Where I think this needs to go is kind of the direction of the consent receipt is to standardize it across domains.

So, I think it's absolutely great that in some spaces where we're seeing that...in some spaces and in a lot of the discussions I've had in the healthcare space people say, well, an OAuth decision that's not consent, the user is authenticated in making a conscious decision and they're informed but that's not consent because that's...we don't know why but it's not. And so that is...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Well, I should add that the definition of consent and one of the things that we've run across is the definition of consent, at least in the health space, is different from state-to-state.

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

Yes.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

So, it's not really people's opinion in many times it is codified by law like the State of Texas's law about informed, you know, they have a very definite definition. So, law does come into play as well here it's not just, you know, people being...you know, trying to continue to do what they've been doing it's also health law which can be very complex. Are there other comments or questions?

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

I was just going to say not only complex but it also tends to lag as we see...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah.

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

The HIPAA definition of even requesting access let alone getting notification and consent its written even in the latest update which I think is what 2005 something like that, it's written around the paper system.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

You mean the HIPAA?

**M**

Yes.

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

Yes, HIPAA.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah, but then the state law.

**M**

...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah, HIPAA doesn't supersede state law that's stricter...

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

Right.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

So, that's where you...who is that? Is that Aaron trying to...

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

Dixie?

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah?

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

This is Jeff Brandt again, I do have one other question for Justin. When I attended the Blue Button developer conference in San Francisco, last year or the year before I can't remember now, they talked a lot about trust bundles, is that now gone because of OAuth?

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

So, trust bundles are something that are very specific to the Direct Project because the Direct Project makes its trust decisions based on certificate authorities and sort of...

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

No I agree, I agree.

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

...PKI.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

I agree.

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

So, if I may finish the thought.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

Yes, I'm sorry, I'm sorry.

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

It's okay, I don't think that they're necessarily gone as much as it doesn't make as much sense to apply the notion of a trust bundle in the way that it's defined at the...in the Direct Project you don't need it as much.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

I agree.

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

You do however need to have a trust anchor of some type. Now that anchor could be at several different levels, it could be in the patient themselves and their "I just trust this App because I just wrote it and therefore I trust it to get stuff." That should be good enough for some use cases.

It could be I downloaded this from the App store and it's registered in a registry that my provider has decided to trust through certain sets of contractual obligations then that's another level of trust. We tried to capture and codify that a little bit.

And we originally were calling the Blue Button Plus registry a trust bundle server but the Direct Project guys yelled at us for that...

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

Oh, that's the...

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

So we changed it.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC**

That makes sense. I appreciate it, I understand now so that really...because of OAuth and I understand that too and it does make sense so it's been deprecated, okay, I understand, thank you.

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

Yes.

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

This is Peter, I'd like to ask a couple of questions that are going to seem very elementary but I just want to make sure I got this correct because I've seen this a couple of times and I think that this time I actually got some of it. A lot of this stuff has always made me feel like I was not qualified to be on this committee.

So, OAuth 2 is basically a standard for an individual center storing an authorization, writes delegation, basically an identity and it's kind of local where OpenID Connect is a framework for federated sharing of OAuth 2. Is that correct?

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

Not quite, I'm just trying to decide which thread to pull. OAuth is really fundamentally a delegation and authorization protocol it on its own doesn't actually say anything about identity. The client application might not have any idea of the identity of the user all they know is that, you know, I popped open a browser page and somehow I got something back that lets me access an API that doesn't actually tell me who said that.

So, what OpenID Connect does is it defines that API and it says that if you get back this piece of information you can trade it for something a token, an access to an API that tells you who said so which ultimately gives you this federated login capability.

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

But where does it get who said so if who said so isn't in OAuth 2?

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

Ah, that's a great question. So, the resource owner, which is the generic term it's usually an end-user of some type, has to be authenticated somehow to the authorization server at the point of the authorization request. So, when the client pops open that browser and sends the user over to the authorization server the user then has to authenticate to the authorization server using some mechanism that the authorization server wants to do.

Now at this point this could be as simple as a user name and password, it could be multifactor, it could be certificates and hard tokens, it really could be just about anything, it could be another federated identity protocol that lets you in.

But before that authorization decision is allowed to be made the resource owner has to be authenticated to the authorization server because only then does the authorization server know that whoever is showing up in the browser at the authorization end-point is even allowed to answer this question of “can I give this client access.”

And additionally, usually who says that, you know, who authorizes the client limits what the client has access to when that token finally comes back down the other end.

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

Now is that coming through OpenID Connect or OAuth 2 or neither?

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

The more general answer is neither. So, that identity information is between the end-user and the authorization server.

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

So, why do we need OAuth at all? Why isn't it just OpenID Connect connecting whatever the authorization servers are doing?

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

So, as a matter of fact, a lot of people are deploying OpenID Connect and OAuth using the same infrastructure because you can. The biggest thing is that OpenID Connect defines a specific API to access and is an identity API. In order to access sort of more generic resources that are not identity related such as your health record, for example, that's when you need the more general OAuth.

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

Got it. Okay. I had one other question.

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

Sure.

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

Which is related to the consent. There are a fair number of physicians I know that are doing complicated and critical things like neurosurgery that are videotaping their consent. Are you saying that is not a HIPAA approved form of consent because it is not paper and it is not signed but it's videotaped?

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

I am not a lawyer so I will not answer that on record.

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

As far as you...okay, as a non-legal...

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

As a non...

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

Question though that seems to be the case.

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

It does seem to be the case but the thing is it very obviously does comply with the spirit of the law so in my view it would pretty easily hold up, but again, please don't base your, you know, your legal...don't take this as legal advice.

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

Gee, I wish I had videotaped of this conversation.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

That's a different consent, Peter, that's informed consent for treatment that you're talking about and HIPAA doesn't even address that.

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

That's a good point.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

That's an absolutely different set of laws.

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

Okay.

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

Yeah, Dixie, makes a point so those might be written a little bit differently. Basically, when I went and read HIPAA, and again, not a lawyer, so I was kind of scratching my head at a lot of it, the impression I got was that it was very much written for a paper-based system which is exactly what existed at the time that HIPAA was invented. So, it makes sense. So, I'm not saying we need to throw away HIPAA not at all, I'm saying we need to sort of bring HIPAA in line with the times.

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

Well, I disagree with you because medical organizations were exempt from HIPAA if they were not using electronic systems. If they had no connectivity over electronic systems they were exempt from HIPAA. So, it was written at a time of a paper-based system but it was certainly written with the electronic systems in mind.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yeah, it included the digital signature at the time which you'll recall was taken off the table because of privacy issues.

Okay, we're coming up on the time when we need to really wrap up and talk about the next steps. So, are there any other questions, you know, burning questions that you want to ask Justin. You also see his e-mail there so, you know, I'm sure he'd be happy to follow-up with you as well.

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

I would.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

If there are any questions that you really want to get in this discussion please come up with it right now so we can...

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

This is Brian Freedman.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Hi Brian.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

I just want to real quickly say, I mean, just listening to this it's...you know, you made a great point about, you know, what Facebook has kind of done, so from a consumer perspective right now I'm asked to log into like five different medical portals. So, the idea is that this would make it so that I could log in once somewhere and be able to access...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Holy cow.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

...

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Somebody opened...

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

I'm sorry there is some obstruction or something. Go ahead?

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

As long as the EHR vendor, you know, implements it I guess than, you know, you could have that ability. Is that correct? Is that kind of part of the spirit of this?

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

Yeah, as long as they implement it and they trust it in the appropriate way and this is one of the tricky things with this is that a lot of people see a protocol like OpenID Connect and they say "oh, it gives me your name and e-mail address" so that means that when you show up with something that claims a particular name and e-mail address then I have to trust those values and use those to look up your medical record.

So, you know, Dixie goes in and logs into her doctor and she has a Google account that says "Dixie Baker" and so it pulls up the first Dixie Baker record and people see that and say "like, no that's ludicrous we could never do that" and I couldn't agree more.

The thing is you shouldn't actually need to trust any of those attributes to have a very strong binding to any particular record. And this is one of the things that we really need to figure out how best to do this in the healthcare space so that for example, just picking on Dixie again, she could go to her doctor and say, you know, like, hi, doctor you know who I am, you know which medical record represents me. I am going to log in right here and now to this system with my digital identity that I am asserting is me and I can prove that I have control over and allow you the doctor to bind that digital identity to that particular record in a very trusted and very well vetted fashion.

And so, ultimately, I know this is a roundabout way to answer your question, from a technological perspective, yes, if they all just turned on OpenID Connect it would just work. The problem comes with the trust and the policy and a lot of systems are not really set up with a federated or externalized identity and credential set in mind. And I think we need to go there.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Yeah, I agree, well, yeah, thank you very much.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Yes, and thank you Justin, thank you again, we really appreciate your taking the time to meet with us and you just do a fabulous job so we really appreciate it.

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

Well, thank you for having me.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

And as for next steps, the next meeting is in two weeks and as both Justin and I said that should be a very, very interesting conversation with Eve Maler about the User Managed Access profile which is a profile of OAuth 2 so it builds upon what you heard today. Okay with that is there anything else you want to add Lisa?

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

No, Dixie, thank you.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Okay, so I think we're probably ready for public comment.

**Public Comment**

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

Operator can you please open the lines?

**Lonnie Moore – Meetings Coordinator – Altarum Institute**

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. If you are on the phone and would like to make a public comment please press \*1 at this time, thank you.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**

We have no public comment. So, thank you everyone and our next meeting will be in two weeks. Have a wonderful rest of the day.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Thank you again.

**M**

Thanks, Dixie.

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

Bye everyone.

**M**

Thanks.

**Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates**

Bye-bye.

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

Bye.

**Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society**

Bye.

**M**

Bye.

**Public Comment Received During the Meeting**

1. Need to have properly placed incentives for enabling the Sharing of Data. Often "consent" entails the documentation of a Discussion with the Patient and with the Provider. The key word is "discussion"