



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
October 22, 2014**

Presentation

Operator

All lines are bridged with the public.

Michelle Consolazio, MPH – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology

Thanks LaTonya. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the HIT Standards Committee's Transport & 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 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.
Hello, here.

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

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC
I’m here.

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

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC
Hello.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District
I’m here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, John. Lee Jones?

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

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

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

How are you?

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

Good, thanks. Paul Clip?

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Yes, present and...

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

Hi, Paul.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

...maybe I should...

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

Not yet, Paul.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Nope.

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

Peter Kaufman? Scott Rea, Scott Rea, I'm sorry? Sharon Terry? 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

And Mazen, are you on as well?

Mazen Yacoub, MBA – Healthcare Management Consultant

Yes, I am, sorry, I was muted.

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

Okay...hi, Mazen. With that, I'll turn it over to Dixie and Lisa and also quickly note, and I'll let you decide, Dixie, Paul Clip has joined the group and so you may want to let him introduce himself as well.

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

Okay. Okay, now is Eve Maler on yet?

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

She is on.

Eve Maler – Vice President Innovation & Emerging Technology - ForgeRock

I am here, yes.

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

Ah, good. Hi, Eve.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Hello.

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

We're practically roommates these days.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

I know it's nice to hear your voice again.

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

Yeah, nice to hear your voice, too. Okay, this is Dixie Baker and I'd like to welcome you all to the meeting of the Transport & Security Standards working group and extend my thanks, along with ONC's for taking the time in I'm sure what all of you have are very busy work schedules to participate in this working group. It's only as good as the inputs that we receive, so we really, really appreciate your dialing in and your participation.

Today's agenda, we're going to...there are actually two main parts. Last week, last Wednesday was the monthly meeting of the Health Information Technology Standards Committee and for the first time ever, it was a joint meeting of both the HIT Standards Committee and the HIT Policy Committee. And it was a long meeting and a very, very productive meeting and there was very high participation, even though it was a very large group. And so we're going to go over some of the key points that were made and then Lisa and I will give you our observations on things that we picked up as the day progressed.

Then we'll move into the highlight, the guest presentation for the day is with Eve Maler who chairs the User Managed Access Working Group that's developing a profile of the OAuth 2 standard. And this profile, this UMA profile that she will describe is very relevant to one of the tasks that we have for this year, which is to recommend some standards around the management of user consent...of individual consent, not user c...individual consent. We'll leave time at the end for...we'll have questions and answers after Eve's presentation and then we'll leave time for discussion of next steps and public comment at the end.

I would remind all of you, as one of you just reminded me, when you speak, do make sure you state your name because this is a public meeting so we want to make sure that the public is aware of who is speaking at all times. Okay, Lisa, do you want to add anything there?

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

No, I think you covered it well, Dixie and I'm looking forward to the discussion.

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

Okay, then let's go to the slides that present the high points of the HIT Standards and Policy meeting that was held last week, last Wednesday. There were several presentations during the day and several of them, three presentations really related to the roadmap that the ONC is putting together, and they all related to the current draft of the roadmap. And ONC was very clear to make sure that we understood that, that this is the initial public view of what they're working on, but they clearly were soliciting inputs from us for the roadmap, and they certainly got them.

So between the roadmap and then there was a presentation of the JASON Task Force, which is the ONC's task force that they put together to develop a response to a JASON Report that came out several months ago. And so that was the final presentation of the JASON Task Force's recommendations on how we react to the JASON Report. And JASON is a group that I guess is, you can look it up on Wikipedia because it's quite interesting, it's a group that really is not at least publically it's not sponsored by any one organization but it's a group of experts in various fields who come together and write these reports and give advice to various industries and they did give advice on architecture for a National Healthcare System and this was the task force that responded to it.

So if you look at the slide that's displayed on...let me see, is it displayed on my screen yet? Let me go back here, yes, is the roadmap presentation presented both, one of the presentations was about the context for the roadmap, what they were trying to achieve, another was about governance, which in my personal opinion, is the most difficult part of all of it and I think that we heard that from the audience as well. And each of a number of areas they presented some sample draft action plans. The one that...and we'll just show you a couple of them, this one is the architecture and standards action plan.

And you can see the level of detail that they went into around architecture, around architecture and standards. And their recommendation here is quite consistent on what both the NwHIN Power Team and the JASON Task Force preliminary recommendations came up with is to really focus a conscientious effort on refining and constraining the consolidated clinical data architecture specification. Go to the next slide, please.

This is the core functions around, which area, is this...oh, these are the ones for security, and these are the core functions for security, yeah. I think, let me see...I made a note of what the core functions are, identity management, which is something that we will be working with and the other area was provider identity management. So these were two actions that were recommended, I'm not sure in which area they were recommended, actually, but they certainly do cross what we've been asked to do. The next slide, please.

This is from the JASON Task Force. The recommendations, these are the final recommendations from the task force. One is that ONC and CMS should align the Meaningful Use Program to focus on expanding interoperability through the use of public APIs. And they stressed that there should be, right

now we have multiple application programming interfaces and we really should...multiple, purpose specific and what we need is a single, uniform API that can be profiled for specific purposes, but basically would be the same transport and security in that API and basic standard for the vocabulary and the containers of information as well. The JASON Task Force recommend a market-based exchange architecture be defined, and the core of it was this public API that they recommended be based on some...be RESTful and that it be based on something like FHIR. They came...I think they came short of recommending FHIR, but that's...HL7's FHIR emerging standard. The "loosely coupled" relates to that there really shouldn't be any co-dependencies that prevent nationwide interoperability, but rather it should be loosely coupled to encourage nationwide sharing. Next slide, I think there are two more, yeah, three more.

The public API should, and they meant by public they meant not proprietary, that doesn't...and they were clear to point this out that that doesn't mean that the public could use it, anybody could use it, but rather that it would be not proprietary and not just government, but public and private sector as well as not proprietary, and it should enable both...let me, hold on just a...sorry, my phone was on the other side of the room, but it rang anyway. It should enable both data and document level access, in other words, exchange of Consolidated CDAs, but also being able to query for discrete data elements, like being able to go in and say, let me see the result of the blood test that was performed on Joe Jackson last Wednesday. The core data services and profiles should define the minimal data and document types supported by the public APIs. And ONC should assertively monitor the progress on it.

Now, I wanted to make a couple, for Lisa and I asked Lisa to this as well, make a couple of comments back on the roadmap. They emphasized that this was an early draft report, as I mentioned. They started off presenting 11 learning health system requirements and of those...and the whole roadmap really is geared toward moving us toward a learning health system where we have continuous improvement and feedback and the use of data so that we can measure outcomes and improve based on real objective measures of results.

So the learning health system requirements listed 11 requirements and 7 of those 11 relate directly to security and privacy. And those 7, I'll go over are ubiquitous secure network infrastructure, consistent secure transport techniques, standard secure services, accurate identity matching, consistent representation of individual interests in sharing ones data, in other words consent, permissions, whatever you want to call it; verifiable identity and authentication of all participants and consistent representation of authorization to access data or services. And I wanted to note that a number of the tasks that we're undertaking this year relate to those objectives including standards for authentication and authorization and identity management, as well as standards for consent management.

The privacy and security building block that they presented had a sample 3-year action plan. I think this is...and it was similar to what was shown in that earlier slide, but the one for privacy and security said that ONC and stakeholders should develop methods for consistently representing, managing and communicating privacy preferences and consent. And the other one was that stakeholders consistently implement security best practices including encryption for all information at rest and in motion. So those were the sample building block action.

They went over a number of draft milestones and building blocks for the learning health system. I thought it was interesting, and this also relates...I tried to pull out things that relate to our tasks, our work plan tasks. They considered the Data Segmentation for Privacy a current standard that needed to be maintained and improved, which said to me that it prob...we're likely to see that in the 2015

Certification NPRM. The standards that needed to be curated and refined included patient consent, RESTful web services using OAuth 2 and OpenID Connect, which we'll be talking about today, data provenance, individual matching and genomic and other –omic areas.

The privacy and security building block which they included looked really good to me, I was really impressed and I mentioned this to Lisa and she said, oh well, she had had major input into it, so we can thank Lisa that the privacy and security building block really looks very sound. And I specifically noticed that it extended the focus not just on EHR, but also to public health and to protecting the national critic...and health as part of a national critical infrastructure. So those were just the comments that I personally wanted to extend...to share with all of you, because they so...they most relate to what we've been asked to do.

Lisa, would you like to make some comments about the meeting?

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

Yeah, I think the meeting, as you said Dixie, we covered the three major areas, governance...well the Interoperability Roadmap, the Governance Task Force recommendations as well as the JASON Task Force recommendations. I think as we go forward in this discussion today and in the future, we are going to...you'll see clear mappings between, as Dixie tried to introduce here, between what has been discussed in other federal advisory committee task forces and workgroups, what has been presented by ONC and the interoperability team and our work plan going forward.

So, Dixie and I, along with ONC and our MITRE support staff are really working to make those connections and to make the work that we do extremely relevant and mappable to the progress that we need to make as an industry going forward in the next year. And so we're looking forward to that, we're looking forward to your feedback and input and your participation. We will have quite a list of interesting topics to work on and recommendations to make. So from here forward, I think will be your opportunity to begin contributing and helping us create those recommendations and have an impact on this roadmap and facilitating interoperability. That's really all I wanted to add.

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

Thank you, thank you, Lisa. Are there any questions or discussion of...some of you may have dialed into the meeting last week, you might have other points you want to bring up, please feel free to do so. So let's just open the floor for any additional questions or comments.

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

Hey Dixie, I have a question. This is Aaron Miri at Children's and I appreciate very much the overview of the meeting and your observations and notes basically, that's very helpful and matches very clearly with all of the publications and secondary commentary I heard from other sources related to the meeting. Everybody seemed very positive from the outcome and that's exciting.

My question to you is this, as a provider perspective, one of the most difficult things is again, I kind of spoke to this in our last meeting, that carrot for me to exchange data and for me to even want to go down this path. Did the ONC or was there any talk on the roadmap of how they're going to try to entice organizations to share data knowing they obviously have to be respectful of HIPAA and everything else but that if you don't do something 100% correct, but your intentions are well mattered and you tried your best, that you're not going to have the OCR knock on your door. Was there any discussion about that because there seems to be a little bit of a conflict in methodology depending on what federal

agency you're speaking with as to, can I share data? Can I not share data? If I share data inappropriately even though I meant well by it and I made an innocent mistake I'm going to be penalized millions of dollars, was there any discussion around that?

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

I...they...during the governance presentation they talked about incentives, so...to share. But they really didn't talk about security oversight and how it might be factored into the whole thing or I certainly...Lisa, did you hear anything on that?

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

No, I didn't and I think this is something that as we go forward, we should encourage them to work with OCR to get some understanding of what an organization needs to do in order to be clear on how and when and under what circumstances they can share data. Keep in mind, too that we still don't have guidance on minimum necessary from OCR. We have a number of areas where they could provide us additional guidance and tools and resources to help make those kinds of decisions.

As far as incentives I would say that because there is some discussion about proactive incentives, but there's also, you know, the notion that as we move to new payment models and new ways to collect, analyze data and be paid for quality outcomes, that some of that will come organically. But as we go forward with regard to the governance building block, I think there will be quite a bit of focus on how we facilitate or how we incent providers to participate, and I think that's something that we can continue to follow from the governance workgroup and from the activities...from the document that ONC will put out in January, the 1.0 version of the roadmap.

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

Yeah.

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

All right.

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

I think your point about the security aspect and what you can safely share under what circumstances is a really excellent point and I think continuing to work with OCR to try to clarify that is something that we should think about, Dixie.

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

Yeah, personally I would...Julie, I'd like us to talk about how...I think that's a really, really good point, Aaron and I would like to discuss how we can get that point in front of the people who are still working on the roadmap around governance. Because they're trying very, very hard to come up with governance approaches that will not only enable sharing but will encourage sharing and I think that they would welcome a comment like that as an area they could look at to really make it...that's a barrier they could address. So Julie, let's put that on the list to follow up on.

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 made a note of it, Dixie.

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

And I’m happy to help lend a voice however I can from a provider perspective. However I can assist.

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

I think I’d have Julie figure out how to do it and ask you to write up a paragraph for us, to make sure that we do express it in the right way.

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

Yes.

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

Thank you.

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

Others? Thank you very much, I appreciate it. Other comments? Okay, well if there are no other comments, let’s just move ahead to our presentation by Eve Maler. Eve presented this UMA to another group that I’m associated with on Sunday, so I should have it memorized by the end of today. So thank you very much, I know that Eve is stretched very thin, a lot of people are looking at this profile and we really appreciate you giving us some of your time, Eve.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

It’s my great pleasure. So yeah, Dixie, you’ll have memorized these slides. I guess I’ll be doing the next slide please gambit today, right, with you guys are controlling them.

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

Yes.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So ere you see my affiliations, the most important affiliation for the purpose of today’s presentation is actually that I actually run the User Managed Access Working Group and I will be telling you about the work at the standard protocol today. So if you’ll proceed to the next slide, please.

I want to start by talking about actually the problem space around online applications that handle PII of various sorts. In this case, what most interests us is health-related data. So next slide, please. When you think about applications collecting data and really touching data, a lot of times the way that the data gets into the system is oft times by asking a person to input the data, as we say by hand and by value and I refer to this as the Web 1.0, dark ages. And the reason that it’s so undesirable is that it’s inefficient for the person, it’s annoying for the person. It often times when you ask for data that they’re uncomfortable giving, they are not happy doing that.

Often times when you ask for data that you didn’t strictly need, for example, for marketing purposes which sometimes even EHR systems can do, people will...they’ll try and get away with lying to you, so

you don't get very good data. And, when you actually store data by value, meaning the actual...if you think of data that is not sourced from an authoritative source like, for example, the National Change of Address Database if you want to know somebody's actual address, what you find is that somebody moves and now the data that you spent a lot of money storing, goes out of date. So we've got a number of problems with this model of data-sharing. Next slide, please.

We actually had kind of a revolution of sorts quite a few years ago with a model that's used in the financial applications of the world, if anybody's familiar with the Mint.com model, where Mint actually asks you to input your user name and password for a bunch of different systems so that improves on your putting the data in by hand, but it means that you're putting in your credentials by hand and it stores those credentials and then goes out and gets the feed of your bank account data. So this gets to financial data, it's not health data, but you can imagine how it's sewing together a series of application-to-application connections so that it can download the data and that way it's getting that fresh feed that we want.

So it fixes a problem, but it creates a new problem in that we've now just shared somebody's password, which is just bad security practice. So this is known, in fact, as the password anti-pattern. And so that means that passwords are stored all over the place and the password for, let's say, your Bank of America account is now, well it's not secret to you and Bank of America that's just bad. And the banks, I can tell you, don't like it and anybody dealing with health data is probably in violation of a whole bunch of laws if they even encourage this. And it's actually hard to stop third party applications from doing this. So, we've got a number of problems we just gained in solving one problem of getting those fresh feeds of data. Next slide, please.

Now this is where the OAuth technology that I know you guys are familiar with came into play, it was actually invented in main to solve the password anti-pattern. So, this is a screen shot showing an example of an application that happens to connect Twitter. And the way you're probably familiar with it working is, it doesn't collect your user name and password from Twitter, so the third party App does not see your credentials at the main site or the main application, it sends you over, it redirects you to that application to go log in and crucially, to consent, to authorize, as you can see here, the third party Apps to connect.

And what that third party App gets instead of your user name and password is an access token meant just for it with power maybe to just do something limited at that API. So if you imagine a health API like FHIR or like some others, it could use this OAuth pattern to actually achieve a kind of delegated constrained access to these client applications and that's improved because we've now collected consent at the right place, we haven't displayed passwords all over a bunch of systems that shouldn't know them, but one-time consent is actually kind of weak.

So if you go to the next slide, please, you can see somebody's imagined version of the problem with one-time consent, which is, it comes at the wrong time because the two applications in question have figured out what they need to know from you. And this is true even if supposedly upstanding citizens like EHR vendors, hospital systems, they're going to try and get data from people that may help them in their own business purposes and those people are going to be incentivized at that moment to say yes, to get on with it. And so one-time consent is actually a very weak form of privacy management, nonetheless OAuth and its OpenID Connect cousin are friendly to the revocation whenever the user wants, of that access between applications. So it's kind of got one foot in some pretty good, robust privacy and one foot in well, at least it collects consent, which is nice.

Next slide, please. So that's all application-to-application data –sharing, which is great. So if we have, let's say a patient, an individual named Alice, she's now shared data with herself using two different applications. What about Alice to Bob sharing? It turns out we actually do this all the time. If you use Tripit or if you use Google Docs, which I do a gazillion times a day, or if you use Flickr to share photos, there are patterns of usage where we share data with people or companies or whatever, who are not us, other autonomous entities with whom we do not share credentials at all. We desire to share access with them proactively for our very own purposes. So there's a very well-known pattern of proactive sharing desire and proactive sharing usage. Next slide, please.

How do we actually solve that problem today if you look at the applications, the online systems of our acquaintance? Well, if you look at Google, well, the property that it has called YouTube, one of the ways it does it is to share what it calls a private URL or an unlisted video with a secret URL. And you can see there that it says "only those with the link to this video can see it." It turns out that's a fairly weak security way of sharing with another person or another system or another organization, maybe with a doctor, something that's sensitive. It's okay maybe for my barbershop chorus, which is what you're seeing here, it's not actually good for anything truly sensitive, so I think we can just cross that off the list as a solution. Next slide, please.

We do have a good example of somebody who has gone off and implemented a very nice, but very proprietary access management system for sharing between autonomous entities that do not share credentials, and that's Google in its Google Apps System. And so if anybody actually uses that, you're probably very familiar with this pop-up where you see you've got a document with a unique URL and even if that URL were to get out into the wild, not everybody in the world could get access to it. In fact, you need to be logged in to the Google System with the right email address essentially, to get access based on the configuration that you see here.

What you see here is actually access policy. You could think of it in healthcare terms as a consent directive. In fact, in HL7 terms, think view, download, transmit rather than this dropdown of is owner, can edit, can comment, can view and you can think of that how it should look if this weren't a proprietary system. Next slide, please.

Now the other way that we see this solved unfortunately is not so great. If you go look at the Fidelity.com website and you see its instructions for how Fidelity Bank data should be shared with your tax preparer in Turbo Tax, so even if that tax preparer isn't you, they basically say, yeah, put in the username and password, so we're back to impersonation again. So even in a person-to-person scenario, as we often see with tax preparation, tax return preparation, we're back to this crazy thing of username and password scraping and fading and password vaulting and replaying. So those are kind of the ways we solve this today. Next slide, please.

It turns out that this impersonation thing really does need to be solved because, as we know, strong authentication it's, I mean, sounds crazy for me to say, it's the way of the future. People talk about killing the password, I'm on record in my former analyst role at Forrester as saying, I don't think you can kill a whole authentication factor, but, it's demonstrably true in our daily lives that second factors of authentication are getting added to things we do. And anytime you even add the simplest thing like texting a one-time password to your phone in addition to a password, for example, it completely destroyed the value of password vaulting.

And then this example on the right that I show here is this cool thing where it's an electrocardiogram means of biometric authentication where you wear a little wearable, fitness wearable type thing, and that's coming on the market now. It's in beta. So, you can clearly see that password vaulting is about to be kind of crossed off the list as something viable in the very near future as working for person-to-person sharing as well; so given that, we really need constrained, delegated authorization even for entity to autonomous entity sharing, if you will. Next slide, please.

So, we have some pretty stringent requirements we have to solve. We know it has to be lightweight for developers, we can see that through the RESTful Initiatives in healthcare that are being so effective because they're focusing on those wonderful objectives of things like rough consensus and running code and iteration and agility. It has to be robustly secure; we have to cross off of the list any solution that depends on things like security through obscurity. It has to be robustly privacy enhancing, it can't just rely on things that we know and are sort of modern era are inherently weak methods of privacy. They have to be, in our case, patient-centric, individual-centric.

They have to be Internet scalable, so they have to be responsive to a kind of a continuum of Web to mobile to API to Internet of things where, for example, medical devices are already all over the place. They have to be multi-party in the sense that we have way too many use cases already where it isn't just sewing together applications to share data, it's sewing together people who want to share with other people and organizations, particularly when we're looking at public health use cases where we want to incentivize people to share data of their own, so personal health data, kind of for the greater good. This is what we were talking about at the Genomics Alliance with the use case of incentivizing people to share data because there's a mild upside for them in helping society, in fact. And so there are a lot of use cases like that. And then finally, if it's not convenient, it's not going to be viable. All right, next slide please.

So with those in mind, I would like to introduce you to UMA, and I use this picture because it's got Alice and it's got Bob. Next slide, please. So let me present to you UMA in one slide and then I'll just see if there are any questions so far, because I'm about to get into some technical particulars. So this is a draft standard and you can think of it as being about kind of authorization v.next, you know, the next generation of authorization technology.

We do call it a profile of OAuth, version 2. It's really, you can think of it as a pretty deep application of OAuth that is to say, it uses OAuth and leverages it in a fairly interesting, substantive fashion. Another way of thinking about it is that it defines standardized APIs that do a security mechanism purpose and they have authorization and privacy and consent implications. The work is being done at a particular dot org, it's called the Kantara Initiative which focuses on high quality identity initiatives.

If you're familiar with the XACML technology, which I suspect you are, it's not intended to like kill off XACML or anything, in fact, in many ways its complementary and we very much hope that the various pilot efforts like the VA pilot that I know is under way, that they'll probably end up being very complementary and usable together. I happen to be the founder of the UMA effort, the founding Chair, the current Chair and what some people call the Chief UMANatarian. And it's currently in last call, so we were calling the current version V0.9 and we're planning to head to a finalize V1.0 around the end of Q1 of next year. So while I'm here, let me just see if there are any questions that have been stimulated by all of that so far. Okay, so far so good. In that case, next slide, please.

One of my nicknames is the Queen of Venn, so I have to perpetrate a Venn diagram on you. This diagram shows UMA's relationship to two other technologies that it's in close relationship with. So it has a normative requirement for OAuth at its base. It also has an optional usage of OpenID Connect, which itself depends on OAuth 2. So the three of them together have a nice working relationship, if you will, they're intended to harmonize with each other and it's for this reason that Debbie Bucci and I are actually working to...we're the proposed Co-Chairs of a new group that's intended to get started shortly at the OpenID Foundation called HRT, standing for Health Relationship Trust Working Group. And the purpose of that group is to profile and harmonize specifications for security and interop profiling of OAuth and OpenID Connect and UMA variously for protecting and authorizing access to health data APIs like FHIR. So, we're hoping that next week we will get the word that our charter...our draft charter has been approved by the OpenID Foundation Specs Council, we'll be presenting it to them then. And so roughly at like HIMSS of next year, we'll be presenting a good solid set of draft use cases that will be based on already work that's been done currently. Next slide, please.

I'm slightly regretful of this next slide because, you can go backwards and forward I think, so go one more slide forward so I can just show you the unadulterated diagram for a second. So, the use cases that we're really tackling here are between Alice and Bob sharing. So you see Alice as a resource owner and Bob as a requesting party. So now you can go backwards one, thank you. I sort of exploded these because I know that we don't have animation builds here.

So the use case options that we're solving for here are actually unique, none of those other technologies that were built on solved for that Alice to Bob piece, so that's unique to UMA. So the goal is to enable Alice to share data and content that is hers that she either created or that's about her selectively, meaning not publically, whether it's with her own Apps, with family and friends, with organizations, with her doctors, with could be research organizations. Another way of seeing the use case is, she wants to protect this stuff, she is not one of those TMI people, she is not...she is afraid of what gets out on the Internet and she wants to have a level of comfort about sharing it. And then finally, Alice wants to control access proactively not just be presented with that I agree button or the I authorize button over and over, because that doesn't feel like privacy. Next slide, please.

So digging just a little bit deeper into how this works, what you're seeing here, these little bubbles on the screen, most of them are actually, the terminology mostly comes from OAuth, so "resource owner" is an OAuth term, and I'm not actually crazy about the word owner, because when it comes to property rights, owner is complicated. But, okay go with me here, this comes from OAuth, and most particularly resource server and authorization server are two key concepts in OAuth. And what we're doing most especially in UMA, is to make that authorization server function, be presentable kind of like a SAS service, so think authorization as a service. Now I know a lot of you are going to be familiar with federated identity single sign-on, so, go to the next slide, please.

A resource server could have anything, it presents any API. But one of the jobs that's really not the core competency of let's say a resource server presenting a FHIR API is how it protects those resources. So UMA gives it the opportunity to literally outsource protection of those resources to some central authorization or think of it as a consent server. And that central server, the authorization server, has standardized APIs that serve a privacy and a selective sharing function and that gives Alice the opportunity to go to one place, this is subject to business models to a certain extent, but go to one place to set those sharing preferences for convenience and better, more robust security, better, more robust auditing, better, more robust revocation capabilities if something goes wrong. Next slide, please.

So, you can think of the resource server as kind of playing a role like a relying party in single sign-on, except that what it's relying on is authorization instead of authentication. Next slide, please. And you can think of the authorization server as playing a role much like an identity provider only what it's providing is authorization. So it's very akin to federated identity, only its federated authorization. So I've invented these little AzRP and AzP terms kind of like an RP and an IDP. I don't know if that helps you, it helps some people I think. Next slide, please.

So just to sort of roll this all up, we're talking here about a number of healthcare use cases, but a mechanism like this would actually not be very useful if it were only applicable to healthcare because centralizability is actually a benefit to Alice, whatever she's protecting, whatever data she's protecting in her life. And we can see that in healthcare because you look at the quantified self-movement, you look at fitness wearables, you look at things that start to edge away from sort of pure healthcare, they may yet be regulated or as things start to edge away and start to be just for fun, maybe they're sports related, now you go into something entirely different.

Maybe she goes for runs with her dog and her dog has an Internet connected chip and before you know it, lots and lots of sources of data are things that she may want to aggregate and track and run analytics over and it's not really sort of for us to say. So we want the opportunity for her to protect that data, have consented permission sharing over it, regardless of its source, in fact. So the fact that this applies to health data, to tax data, to small business managing your books data to eTranscripts from higher education; I've talked to folks who want to use it for lower education, for managing school work and immunization schedules as kids head to the school year, to calendar data. So this is interacting with government agencies sharing attributes on that basis.

I've talked to enterprises who are interested to use this to manage the selling to digital subscribers of digital media that they stream and download. And behavioral is meant to evoke some targeted marketing. If you know the geo-location for example of your Telco subscribers, that's the kind of data that you may want them to permission you to know, so that you can maybe offer them better deals in the geo-fenced fashion, for example. Next slide, please.

So that's kind of a vertical...industry vertical view and then there's a channel view which is, does this discriminate against any particular channel of data delivery or access to service functionality. And it turns out, as far as we can tell, it doesn't. We've been working on this kind of IoT angle along with the others and its turning out to be quite salutary actually. Next slide, please.

I'm near the end, just so you know. So just to sort of bring it home in terms of the kinds of sharing preferences that our Alice can set, maybe the rightmost example is the most salient for this conversation. If Alice has multiple services that she works with, her health aggregation App, think of like a Mint.com for health, her doctor's office FASS App that lately I'm onboarding to a lot of EHR systems, so I know this pretty well. She might be involved with several of them. She might have a Wi-Fi enabled scale that has an API, she might have a fitness wearable that exposes an API and those need spoked access and she may very well want to permission all of those to...all of those client Apps to read those API's results for various benefits that she herself determines.

So if you think of setting policies like that, what you're seeing is kind of proactively determined consent directives. If you think of consent directives as being something Alice signed and kept on file to determine whether data later generated gets sent out to somebody, then authorization policy residing in a machine-oriented fashion and keeping data from going out until it's permissioned to go out, that's

actually a consent...it's a form of consent, too, only it's proactive. And then you can see these other examples as well; there's a financial example and then kind of an Internet of Things example using my favorite Solar Freakin' Roadways example, don't know if you guys are familiar with that, but I love it.

Very near the end now, next slide, please. So, the question I often get is, well how easy can this be for an average Alice to do? This UMA System does require that our patient, our individual has an online presence. This is a simplifying assumption that we've made. It actually simplifies an awful lot of things. If Alice doesn't have an online presence, then we're back to square one, but assuming that she does, we already know what it looks like to share with others in a robust fashion, we do it all the time, in fact. So that's a great place to start and because we know what it can look like to pre-provision system default policies, policies that make subsequent interactions basically look silent, we think it can actually even be "better than OAuth." For example, if it's me again coming in using a different client application, make it just happen, we can do that, we can actually make it be silent based on policy that I set earlier. Next slide, please.

So if you know the internals of OAuth, I'm just going to spend a moment here talking about what we did to make this happen. The first thing that we did was, in OAuth there is a concept of a resource server and an authorization server, but in fact there are no official protocol arrows between them. What we've done in UMA is define APIs that let the resource server talk to the authorization server's API in a formal, standardized fashion so that it enables any resource server to onboard to any authorization server and any authorization server to accommodate the onboarding of any resource servers so there can be an end-to-end relationship between them. That turns out to be extremely powerful. That's what makes federated authorization happen.

And then finally we added Bob. OAuth turns out not to have the concept of a requesting party at all, so that concept is new and it enables really interesting things. Number one, it means that Alice can share with Bob and number two, it means that Alice does not have to have an online session when Bob uses some application to go and hit the API. She can actually be offline, maybe that means she is sleeping, maybe that means she is passed out in an emergency room, maybe, and no disrespect intended to Alice, maybe she is dead. This enables digital death scenarios so that she can actually pre-provision policies for what happens after she passes, so kind of interesting things there. All right, last couple of slides and then I'll wrap up and take any questions. Next slide, please.

Now there are three technical specs that make up UMA. There's also a kind of a non-technical spec called binding obligations that's actually meant for lawyers, mostly. And what it does is it takes a look at the technical entities in exchange, request and response messages to do this authorization mechanism and it maps them to potentially legally responsible parties that run them.

So for example, the resource owner maps to an authorizing party and the resource server maps to an operator of that resource server and so on, and between every pair of these legally responsible parties, they may obtain new responsibilities between them on the occasion of a particular set of messages being exchanged in the protocol. For example, tokens flow, access tokens flow over the protocol and those are very significant in terms of indicating a responsibility taken.

And so what we've done is define a starter set of what we call binding obligations. And they're the most axiomatic, basic of obligations that you can imagine, but the reason we documented them is, it's a tricky business federating authorization and we wanted to be as clear as possible. We've worked with folks like Tom Smedinghoff and Dazza Greenwood, folks who may be familiar to you, kind of legal eagles who

work with a lot of identity...federated identity trust frameworks. So what we did this for was to underlie trust frameworks of a new kind and we call them access federation trust frameworks.

So, if you'll just go one more slide, you can think of access federation trust frameworks as equivalent to identity federation trust frameworks, but they're not about IDPs and relying parties, they're about these kinds of parties. And that's really a key distinction, all the identity federation stuff that's been written turns out not to obviously apply to an authorization model versus an authentication model, so that's why we put the work into this legal view of UMA. So, last slide. There are a few other sort of back-up slides there if you want to look at the gory details, but I will stop there and be happy to take your questions.

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

Thank you very much Eve, that's...it's a very exciting new profile and it builds nicely...we just last week we heard...or at our last meeting, we heard about OAuth 2 and how it's used in Blue Button Plus, so it builds nicely on what we've heard before. Do I have any questions from the people on the phone?

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

Yes, this is Jeff Brandt, I have a question.

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

Yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Um hmm.

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

Eve, is this an open source product...?

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

The protocol is open, it's open and documented. There are a number of open source implementations of various bits, there's going to be more. On the UMA Wiki home page, there is an implementations page where you can go sort of rummage around and go look at the links to the open source. So there are a variety of choices there, there's one open sourced authorization server and there are a number of choices for kind of software development kits for resource server and clients sample Apps and there is definitely more coming.

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

Jeff, this is not a product at all, this is a standard, it's a profile of a standard, it's a profile of OAuth 2, and so it's not a product at all.

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

Yes, so I...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yeah, I mean there are...just like with OAuth, there are products that implement...

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...yeah, it's similar to that. Yeah.

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

I guess my real question then was, is it patented is the real problem that I'm looking at. Is it a patented entity that you have to...to use.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Oh, you're looking for encumbrances.

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

Yes.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Umm, yeah, oh, I see. I'm sorry, who is this talking, I didn't catch who this is?

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

It's Jeff Brandt. I work with...like some of the guys out at SAIC, which they spun off...that's also under litigation. So, that's why I'm asking.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Oh, I see. Yeah, I mean, so yeah, I can point you to, there's a...as usual with all these things that are developed, there's an IP policy that everything is developed under and we always have these calls for any known IP, so OAuth has a call for known IP and Nokia and others have said, by the way, we have a patent we think is relevant and everybody goes, oh, uh huh, okay. And so OAuth has a couple of those and UMA, to my knowledge, has one of those to date. You can go take a look at it...

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

Okay.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...it's linked from, yeah, the UMA Wiki. So it's sort of...those things are like, I don't know, you have to judge for yourself whether you think that there's a risk of somebody coming after you for licensing revenue I suppose, but...

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

Yeah, I appreciate it.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...in terms of encumbrances, yeah.

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

Thank you.

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

Just a comment...

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

Um hmm.

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

...this is Steven Lane. Eve, I wanted to thank you for your presentation, it was tremendously understandable and digestible even by those of us fairly new to these topics. So, really nice...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Why thank you. We aim to please, thank you very much.

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

I have a question Eve. I know I should have, I guess it was Sunday and I was getting tired, I have a question about enforcement.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Um hmm.

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

An application that makes a service call to the authorization server, is there an assumption that that application will then enforce the permission that it gets back from the authorization server?

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yes, so there's...yeah, this gets to that sort of Cloud authorization model I think we might have been talking about on Sunday. So if you...in the typical OAuth model, this gets into a little bit of philosophy, but in the typical OAuth model, the usual assumption is that the authorization server and the resource server are run by the same company. You can't strictly assume it, but it's the smart way to bet.

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So in that case, you kind of assume well the resource server will respect the scopes and the tokens, so to speak.

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

And a scope is an entitlement, right?

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

Right.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So in UMA, your right to ask that question because we've specifically arranged for them to be able to be run by different companies, essentially...

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

Yeah, right.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...so, and I remember thinking, well that's in contrast to XACML which has a decision and that couldn't happen and XACML puts 100% of the onus on the PDP. And so it does require the resource server, that's partly why we wrote the binding obligations, to put that obligation on the resource server. It is not at the level of technology because you can't.

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

I subsequently found out that even XACML has an out in its...what it calls obligations...

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

Yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...if the PDP hands the PEP something called an obligation, then the PEP is supposed to also do it, but you can't make it do it.

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

Yeah, right. Yeah, that's exactly right, yes.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yeah, so in a way, everything inside that token is an obligation and that's what the binding obligations are meant to do, to a priori bind the resource server by the fact that they're doing UMA because the point is that the scopes are meant to be binding. Although there is, I mean, that's where you could get into something like where an access federation, an umbrella agreement could interestingly specify, all right, what are the ground rules for when you can opt out? Because famously in single sign on, the relying party always has the right to refuse service, so if an IDP says yeah, it's John Doe, I checked him out, it was 9:07 a.m. and I used a smart card to authenticate him so he's good, let him in.

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

The relying party still has the right to go, nah, something smells fishy.

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So you could say that there's always the right of the RS to say no, but you might be able...I don't know the circumstances in which you would say, well, we have the right to let him in even though the AS said no, if that makes any sense.

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

Yeah, yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

But I could imagine an access federation laying out the circumstance, and there are some other subtleties there which I'm kind of hoping we'll get into in this HRT working group because it gets, no pun intended, to the heart of the matter when you've got multiple distributed parties wanting to do the right thing by their own customers and wanting to navigate the liability consequences in a very complex environment. Right?

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

Yeah, exactly. Yeah, you've got the...yeah, yes.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So we're going to hit those, we're going to find that out. I imagine it's going to be on the conservative end and it would rather be, well I'd rather not let them in if it comes down to it.

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

Yeah, I think, yeah...for the rest of you, this HRT thing that she's talking about, she and Debbie Bucci are just starting up, I guess, but it's in the health industry, so what she's saying is that the health industry is very compliance oriented.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yes.

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

So, the health industry is one of the easier places to implement this because there is an inherent tendency to do what's going to keep them in compliance. Yeah, that's a good point, really good point.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Well, I don't know if it's easier, I think that the conservative is like, they're going to be gun shy, I guess or something.

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

Well, there's that, too.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

And so, I'm not sure where it'll come out, but I think that...

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

Yeah, that's...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...current way to bet in that case would be, yeah, would be refusing access just in case, I suppose.

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

Good point. Um hmm. Yeah. Are there other questions or comments?

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

Yeah hi, this is Brian Freedman. So, is the id...like if I'm a consumer, let's say, would...is the idea that at some point there would be some centralized set of resource and authorization servers or for really every different product I might want to use, I might have to go in again and say, well I want to allow him to get this information, but not that information, you know, so on and so forth.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Right. Yeah, and the protocol makes it possible to centralize but business realities sort of dictate how closed or open an ecosystem might be. So if you observe, I've been using Google Apps as an example and that's inherently a closed ecosystem, you can almost think of it as well their trust framework is that they wrote all the Apps, so of course they work beautifully together. But in a healthcare App ecosystem, I think inherently it has to be open, at least in the US market and so that has a number of consequences in terms of like, we're going to probably see more explicit experiences of onboarding Apps to other Apps. My best guess at the moment, for example is, well who might be the identity provider of record in an environment like that? And it would probably be, maybe be the EHR vendors because...

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

Right.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...again my personal experience is, I'm onboarding to so many of these vendors and there are a lot of small vendors, but there are also a lot of big ones and if let's say Cerner already knows me and I have a login to them, why should I have to get another login if I go to the next doctor's practice and they also use Cerner and they have a tenant inside the Cerner SAS App...ummm...

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

That's exactly what my kind of question, that's kind of exactly what I was thinking like if I go to my primary care doctor who has Cerner, but then I go to a specialist that has McKesson...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Right.

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

...hopefully they would...I guess it would be dependent if they want to communicate together or not, I guess.

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

Yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

I mean, yeah. So the more open the ecosystem, the more friction there's going to be for users inherently and the more question there will be about who wants to adopt it and more question about trust frameworks honestly. The more closed the ecosystem, the easier it is to deploy, but then the less centralizable the AS would be and that's where you get into questions of, it starts being higher order

and recursion and turtles all the way down to that oh, now I have policies in an authorization server that I want to export to the new authorization server that I now have to change to. It's like when you change jobs and you change insurance plans and you change...

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

Yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...or you change banks or your bank gets bought by another bank and certain things don't actually get perfectly easy. But, so the protocol supports perfect centralization but real life probably doesn't and I actually don't think that the world will ever get to the point...just like I don't think that human rights should demand us to have a single IDP for everything, I don't think that we should always have necessarily a single AS for everything, but I also think that if we have a chance to pick one, we should be able to.

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

And we should have standards that allow us to understand them, even if they aren't the ones that we adopt.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yes, yeah. Yeah, so like I've talked to a couple of folks who think that there are some home automation players that may be interested to make a bid for, because they're in a position to do some physical authorization of things like groups...

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

Yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...of new IoT things in the home like light bulbs and dishwashers and goodness knows what else, and they kind of want to make a bid also for the logical authorization stuff and while they're not in healthcare, but maybe they would try and make a bid for being the more global AS, maybe.

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

Hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So I kind of don't know how it's going to shake out, but I would sure like there to be a robust, architecturally sound solution for consent and permission and authorization to be ready when and if somebody actually makes a bid for it.

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

And I certainly am looking forward to the day where consents are not a piece of paper that gets filed and put away forever.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yeah, yeah, that's where I'm driving to.

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

Yes. Other questions? Comments?

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Yes, hi, this is Paul Clip.

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

Um hmm.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Hi, just wanted to introduce myself, too, because this is my first call I'm on.

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

Yeah, please take time to do that. Paul Clip is a new member of our working group, so Paul, why don't you start by introducing yourself and then ask your question. My...I shouldn't have...I forgot to say that at the beginning. Please do.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

That's okay. I'm happy to be part of the group. My background is in SAS Apps on the healthcare IT side, worked for RelayHealth, still work for RelayHealth, which is now part of McKesson, for a while, leading their engineering team. And then more recently, have been involved with the CommonWell Health Alliance Initiative and Chair the Standards, Technology and Implementation Group, which are a series of long words we could find the acronym to STIG and that way we can use the Top Gear mascot as our...internal...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Makes me think of the Ruddles.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

So Eve, I very much enjoyed your presentation, I'm just curious about exploring a couple of things. One, the underlying assumption of online presence, is there a case where if a patient would present, let's say we're in the scenario and obviously is not online, so cannot actually serve as the resource owner and give authorization, etcetera, is there a concept that we could create maybe potentially even if we sign...if the patient signs one of those pesky pieces of paper, a default authorization that would either be yes or no either way? You know, deny or approve to get things...?

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Um hmm. Oh, you mean like at the "resource server" you mean?

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Yeah, yeah, someone...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yeah we discussed how, yeah it's kind of a legacy problem in the sense of a lot of these "resource servers" they're just applications which currently do store decentralized policy, right? And so we discussed how there's an opportunity using the communications channel that we built between the RS and the AS to have the RS kind of fill up the AS with the current policy, if you will.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Umm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So that's an opportunity that we have that maybe that comes up in the hard conversation, I'm not sure. But, it is kind of a current circumstance we could maybe take advantage of.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

And presumably the patient, when she comes online later on, could then take advantage of or claim that initial authorization back and basically say, okay, now I'm ready to manage my access to my resources, whether they be...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Yeah, but there are a couple of things, I mean, we're sort of getting a little bit into the weeds of UMA, but basically when the RS on boards to the AS, that represents the resource owner's instruction and permission to outsource detection. And it could be that if there's additional stuff built on top that that is the hook needed to kind of upload the current policy and it may be that that's all just default deny until I go in there and do something...

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Right.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...or it could be quite sophisticated, it could be a bunch of things. But until that connection is made, the RS is free to do anything on its own that it wants to. So that's a kind of a...sort of a current state, future state on boarding.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Okay. And I guess my question related to that and maybe this gets to the requesting party in situations where I can imagine creating, I'm a parent, I could imagine creating a default policy for my child then having the ability to manage that. At some point my child is an adult and then takes over that policy or maybe as a caregiver for my parents, is there a concept of that? Is that the requesting...is that...sorry, the requesting party or is that a completely separate concept from an UMA perspective?

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Um hmm. Well, for somebody who's competent, so somebody who's over say 13 and not...doesn't have Alzheimer's or whatever, they could grant to a requesting party powers, let's say, that are just about as full as they themselves have, the same as you could do in Google Apps. I mean, that's a really good metaphor actually, but for somebody who is not themselves competent to grant that kind of permission, like somebody who is too young or whatever, it's kind of a custodian situation and we've explored that somewhat in terms of the resource owner basically being kind of split, so the person who manages the resources is actually the custodian of the person about whom the data is. And that's where I think our lower education case study may be the most interesting to look at, and that's being done by a fellow in the Netherlands, actually a Dutch lower education use case, K-12 use case. So we could explore that further because I think for say Children's Hospital, it's the parent who has to log in and permission things...

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson
Right.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock
...and so on. So it's really as a stand-in resource owner more than it is a requesting party.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson
Got it. Okay. Thank you.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock
By the way, I'd love to continue these conversations further, please do use my contact information and drop me a note and we could maybe explore further, for any of you who are interested to do so, I'd love that.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson
I guess I just had one more question and...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock
Certainly.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson
...I'm a little surprised you didn't go there, given your first name, but you didn't mention Eve at all? Where does eves...?

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock
The eavesdroppers, yeah, I get that all the time. What about the Trent the trusted third party? So you know, there is...I've spent some time looking at the model of UMA in terms of...we designed it in order to have a nice separation of concerns. So one of the things that you'll, if I had spent the time to like really go into the weeds with the UMA protocol, the resource server, in fact, never gets a chance to see any data about the requesting party, for starters. So the requesting party has the opportunity to provide claims so that the authorization server can assess them in light of policy to see if Bob qualifies in to see...to get access to the resource, but only the AS is actually the one seeing that. And it gets special permission to see that because Bob actually consents to it.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
Um hmm.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson
Yeah.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock
Reciprocally, in the same way that Alice consents to outsource protection, Bob has to consent to the sharing of attributes effectively, for the purpose of authorization. So there's a place where that actually gets consented, so maybe that's of interest to note. The resource server never sees that because it's none of its business and in fact, Alice never really sees that either, so there's a piece of that.

Now in terms of what could be leaked around, we do have some privacy and security considerations documented. Because we're leaning on OAuth and OpenID Connect so much, to a certain extent we share the same threat models...

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Got it, right.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...but there is a little bit of extra threat model because of the opportunity to share with an autonomous third party versus oneself. And so we've accounted for that by suggesting if you're really concerned, there's work going on in OAuth, for example, to go to the proof of possession token versus a bearer token. So we've documented a sort of escalating path that you can take all the way up to the proof of possession token, if you're really concerned about what could happen with what we call a requesting party token, which has some power for Bob to go and get into your stuff.

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Okay.

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

I have a...Dixie again, I have a related question.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Um hmm.

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

I didn't know about the privacy and security...documentation, that's...I'll look at that, it might answer this question. But, obviously a lot of the assurance is directly dependent on how this is implemented and at what layer its implement and how safe the tokens are, etcetera. How do you communicate things like, well, if you'd implement this in hardware its way stronger than if you implement it at the application level and ensure you're...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Honestly, so much of it depends on OAuth, and there's a lot of knowledge now in the world about certain pressure points on OAuth and how it's implemented that there are some best practices and there are some frankly worst practices that the world knows about.

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

Uh huh.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

So we can sort of point to those and there's a huge OAuth Threat Model document, maybe the hugeness is a bad sign, but, I don't know I hear...I talk to some people who are like, uh, it depends on bearer tokens, that's not good enough. I'm like, you do know that 95% of all the SAML done in the world is based on bearer tokens, right? And it's sort of like, you know, we couldn't get anything done if we didn't have bearer tokens in a way, there's mitigations for things like validity periods and so on that we use for those threats. So, but like there's constantly various researchers saying, oh I found this terrible threat that there's risk that you can sort of just hack Facebook and get everybody's everything because they use OAuth.

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

Um hmm.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

And it turns out well, it's either their implementation, which they then go and fix, or it's because of something that's like an unlikely threat because it requires the actual user to be sort of in cahoots with themselves or something. So, there's starting to be some good real world best practice around loss security that we can in part depend on and then there's a little bit extra stuff because of the outlet to Bob...but we do...if you take a look at our security considerations, that's the bulk of it that's interesting right there is that little section about the authorization of a third party and the token, the nature of the power of the token there.

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

And that's where architectural issues are addressed.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Um, well that plus the OAuth Threat Model document which is referenced in that section, I would say.

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

...which also addresses architecture?

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

I mean authorization is funny because it's so high up, I mean it's way up in the App level, right? Authorization is really...

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

No it isn't...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

...semantic stuff. It's really funny...

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

Operating systems do authorization, hardware does authorization, it sends...it isn't automatically high in the stack.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

True, well, I suppose that's true.

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

It's wherever...

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

In this case it's like authorization of API access really is what we're doing, so it's pretty inherently like loosely coupled, and we do want it to be as secure as possible given those interesting circumstances. But in part, that's why we built on something so widely adopted, partly talking about API security on Sunday I think a little bit, people are basing monetization models for the API economy on OAuth, which is a good sign. It's not that anything is perfect, but it's one of the reasons why we based it on that technology knowing that it has the properties of wide usage and...which means that a lot of people have

motivations to fix things when things go wrong and it's been washed through a bunch of those iterations.

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

Yeah, yeah, yeah, good point. Well, I want to thank you for your time and for your knowledge, for sharing your knowledge and this is certainly interesting and certainly is relevant to our work ahead so thank you very much again, Eve.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

You've been so kind, thank you so much. I look forward to any further conversation. Thanks.

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

Okay.

Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock

Bye all.

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

All right, I think we're up to next steps. The ONC and our support from ONC is...ONC's support and Lisa and are finalizing, in the process even as we speak, of finalizing the work plan. So giving...talking to you about the complete work plan will definitely be on the agenda at our next meeting. And you heard a lot about it today, about the kind of things you're likely to see, it's just more the timing and dependencies are more...those will be more of the things that haven't been quite gelled yet. So the next steps, that's the next step and we are in the process of defining what the...what we need for each individual meeting, what the agenda needs to be related to that work plan. Lisa, did you want to say anything more about the next steps?

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

No, I think you covered it. I think at our next meeting we will get into some more detail on the work plan and hopefully all of these informational briefings will help us...help inform those tasks that we have to take on going forward. So thanks, Dixie.

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

Thank you. Okay, Michelle I think we're ready to open the lines for public comment.

Public Comment

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

Thanks, Dixie. 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.

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 we look forward to our next meeting.

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

Thank you.

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

Thanks everyone.