



**HIT Standards Committee
Transport and Security Standards Workgroup
Final Transcript
January 28, 2015**

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 the 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. 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. Boban Jose? Brian Freedman? Jason Taule?

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

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

Jason B. Taule, MS, 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
Jeff Brandt?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture
Hello. Yeah, it's me, hello?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Jeremy Maxwell from ONC? Julie Chua from ONC?

Julie Anne 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
Here.

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

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. LeRoy Jones?

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health
Here.

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

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health

Hi.

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

Peter Kaufman? Scott Rea? 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. From ONC do we have Mazen Yacoub? I know he's on. Anyone else from ONC on the line?

Mazen Yacoub, MBA – Healthcare Management Consultant

Hi, yeah, sorry, I was on mute, I'm here, thanks.

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

With that I'll turn it back to Dixie and Lisa, thank you.

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

Okay, thank you and thank you Michelle, and thank you for everybody for joining the call today. We don't have a long agenda today so hopefully it won't require too much of your time. The last...we've had a couple of meetings about where we've discussed recommendations about RESTful application program and interfaces and security recommendations around RESTful application, APIs.

So, today our primary agenda item is to review those recommendations that were discussed at the last meeting which unfortunately I wasn't able to participate in and, you know, come to consensus on what our recommendations might be.

These recommendations would be presented I believe at the February meeting or would it be the March meeting? Maybe it would be the March meeting I think. Julie, are you on the line?

Julie Anne 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, that's correct anticipated for the March Standards Committee meeting.

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

Okay, so it would be the March meeting is when they would be presented. Okay with that let's go to the next slide. Next slide and the next slide, we have five slides. These...one of the things you'll see is that the, you know...when all was said and done we included...what we recommended were really topics to be considered they weren't really certification criteria and they weren't necessarily standard but they were really along the lines of best practices and so these are the recommendations that, I believe we have two slides of recommendations, and they all have to do with RESTful APIs.

The first one is to use the standard OAuth 2.0 and OpenID Connect which is actually a profile of OAuth 2.0 with transport level security encryption to secure Health IT RESTful APIs. In other words, OAuth 2 as a method to authorize the use of a client to access resources.

The second is to use OAuth 2.0 implementation model, use the implementation model that's most appropriate for the architecture and the risk profile, the application. The OAuth 2.0 specification includes four different implementation flows for implementing OAuth2 and the specification itself indicates the conditions under which you should use each one of them and so this just says, make sure that you've used the...and specification itself also points out the risks associated with using each of the flows and so, you know, it just emphasizes that as you pick the implementation flow to implement that it really should be appropriate for the risks associated with the application.

The third is OpenID Connect enables single sign-on across multiple applications and of course that increases the importance of the strong initial log on. So it becomes even more important to assure that the methods used to initially authenticate the user are sufficiently strong for the application use case. It's a single point of failure problem that we want to make sure that the initial authentication method is strong enough for reusing that authenticated identity.

The fourth is to strengthen client and browser software authentication by using standardized signed web tokens instead of passwords that are transmitted over the Internet and this is a recommendation within the OAuth 2 specification.

And then finally, is to use transport level security TLS encryption with server side authentication to assure the clients that they're communicating with the correct server and to protect data transmitted over the established link.

The way TLS works is that you can use it...well you use it to establish and encrypted link between two ends points and one or both of the end points can be authenticated. So, our recommendation is that at least the server end be authenticated.

So, are there further discussions about these recommendations? Anybody? Okay, let's go to the next slide then.

Okay, I have to bring it up so that I can see it. The next one is a continuation of the first one, is to minimize the risk of data exposure through redirect manipulation by using declared redirect user resource identifiers during client registration.

OAuth 2 works that a client is registered with an authorization server and what this says is that when it registers you should include the complete URI or URL rather than partial URLs.

Establish and enhance the HIT RESTful API security vulnerability testing to minimize evolving cybersecurity threats, risks, test it more.

Ensure that appropriate awareness and mitigation of cross-site API vulnerabilities and the OAuth 2 and OpenID Connect point out a number of these cross-site vulnerabilities where tokens can be reused or tokens can be intercepted within a single enterprise and we're just encouraging them to be aware of these vulnerabilities and threats and to mitigate those threats.

The next one is that vendors should provide customers current information regarding their compatibility in interoperability with browsers and client software platforms and potential impacts on security. We all are all too familiar with this where browsers get out of sync with applications and it does open vulnerabilities. So, vendors should always make sure that they have current information on which browsers they can operate with, interoperate with, securely.

Vendors should incorporate threat monitoring and risk mitigation into the product management lifecycle. There are a number of sources for current risks and mitigation steps that one can take and vendors should be constantly aware, keep up-to-date on those sites.

And then finally, that ONC should track the efforts of the OpenID Foundation HEART Working Group which ONC is involved in, does have representation on, Debbie Bucci is participating on that group and the Argonaut Project both of which are addressing the privacy and security of RESTful HIT APIs.

So, with that can I open it up for any further comments that you might want to make?

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health

Hi, Dixie, this is Lee Jones, I think I have maybe a higher level question. You said at the top that this is not really targeted toward codification inside of, you know, certification criteria or something like that and in the past these kinds of recommendations, maybe not quite as granular, but they were sort of the purview of NIST to make and then ONC and others to sort of point to as best practices. Is that worth something like this would be destined or are we usurping NIST's role in making these kind of recommendations?

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

Well, I certainly hope not, we always do, I mean, we frequently do, I shouldn't say always, but, we frequently do cite NIST guidance on these kinds of things, but I don't believe NIST has specific guidance that address RESTful APIs in the use of OAuth 2.0 at this point.

So, I don't think that there is a single NIST document that we can present, in fact, I think, to my knowledge the best guidance out there at this point is probably some work that MITRE did for the VA and recently made it publically available as guidance. There isn't a single NIST document that we can point to in this arena.

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health

Okay, thank you.

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

Are there other comments? Now one of the things that I thought of as I was reading through, because I've run into this a number of times is, you know, there are a number of libraries out there for implementing OAuth 2 and I think it's become, you know, fairly common practice that implementers just go out and get a library and think they can just kind of drop it in and "there I've got OAuth 2." It seems to me that this might be, you know, a risk, but perhaps we've captured that in these recommendations is to be aware of what you're implementing. Lisa, are you line?

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

Yes, Dixie, I'm on the line and I think your last statement is really exactly why we're doing this so that as we, in the healthcare sector, start to look at the use of RESTful APIs that we're cognizant of all the security guidance and information that's out there and because there isn't one place to point we thought it would be helpful to look at it and to pull it all into one place, this will go to the, I forget the name of the Workgroup that David McCallie...

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

Yeah.

Julie Anne 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

The Architecture...

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

Applications...

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

Architecture Services and API.

Julie Anne 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

And API.

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

Yeah.

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

Right, that Workgroup and we did, you know, we met with the Chairs and they were interested in seeing this input from us. So, I think, you know, we are at a very early stage in this implementation and we are all just really trying to make sure that we have all the considerations in front of us and I think that's where it is right now. So, this would just be some considerations that come from the Transport and Security Workgroup as we, you know, all take a look at RESTful API.

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

You know that does point out that maybe we should...you know, when we present this we should add a slide at the beginning that does explain that context.

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

Yes.

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

Because the Standards Committee won't know any more than Lee how we got to where we are and that it really started out with the application services and API's Workgroup asking us for some guidance and the fact that there is no other single place to go to get this kind of guidance, and that there is a risk that people just go out and drop in the code and that kind of establishes...those three facts kind of establish the context for what we're saying here and I think that would be useful. I think that would be useful so I thank you for pointing that out, Lee, that's a really important point. So, we can work with our ONC team to make sure that we do add that context at the beginning.

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

Yeah, I think that's really important.

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

Yes.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Dixie, this is Jeff Brandt, have we referenced RFC in this document? The RFC 6749?

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

No, I don't think we have and we should, yeah.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Okay, that's the official place for the...framework.

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

Yeah and there's also...let me see, there is...is the threat model a different RFC or is it the same RFC?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

I'm actually not sure.

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

There is...work and then there is...pardon?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

I'm not sure on that one.

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

Because there's also the threat model that might be...but we should get the OAuth 2 both the framework and the threat model because both of those are relevant.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Okay.

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

Good, good, thank you. Are there other comments and suggestions here?

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

This is Aaron, I think it looks good, I mean, I like the suggestions, I like the comments, I mean, it makes sense.

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

Okay, all right, then I think we are...I think we’re set. What we’ll do is we’ll work with the ONC team to add the context before, you know, we may as well wrap this up, you know, ahead of time not wait until March and add the context and also add specific references to the RFCs for both the OAuth 2 framework and the OAuth 2 threat model, okay?

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

That sounds good, Dixie.

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

All right, do we have a short meeting today?

Julie Anne 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

I think so, Dixie, this is Julie. Did you want to just give a head’s up?

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

That’s what I was just thinking we should do, yeah. We were...we decided not to start a new topic because we should be getting, very soon, the roadmap and the strategic plan for review and those are really our next big undertaking for this Workgroup. Maybe, Julie, you could give us some of the timelines for that?

Julie Anne 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

Okay, sure, thanks, Dixie. So, basically we are anticipating information on the interoperability roadmap during the Joint Committee meeting on February 10th so that is something to look forward to and something that would be valuable for the Workgroup members to listen in and/or attend.

And the next thing is the certification NPRM which we don’t have an exact date yet but it is coming so we wanted to let the Workgroup members know to look out for that and that is something that is on the work plan as well.

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

Yeah and those two, the review of that, of both of those is our next major undertaking.

Julie Anne 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.

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

So, that will be coming around next month, we can look forward to that.

Julie Anne 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

Right and I think those were the key updates, Dixie.

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

Okay, thank you and if any of you...I don't know how many of you've dialed into the Standards Committee but Lisa recently led a small task group that addressed provenance, data provenance, and she gave the...presented the results and recommendations from that task group at yesterday's Standards Committee meeting. Would you like to say anything about that? That originally was on this Workgroup's work plan and then it got spun off as a smaller task so that it could be done more quickly. Would you like to kind of summarize that Lisa?

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

Oh, sure, thank you, Dixie. We did form a task group from members of the Standards Committee, members of some of the Workgroups and/or experts from outside of the Standards Committee structure to take a look at this S&I Framework initiative work on a use case for data provenance. This stems from a presentation that the S&I Framework initiative did to the Standards Committee.

The Standards Committee itself had some comments on the use case and recommended a creation of a Task Force. So we started with several artifacts, we had the use case that was approved by the participants in the S&I Framework Data Provenance Initiative, so the use case itself. We had an executive requirements and summary document. We had a briefing from the Chair or the lead person for the initiative, Jonathan Coleman, and we also decided, at our first meeting, that we would have extended public comment from stakeholders and folks working on various standards related projects on data provenance. And we also a member of the Task Force who was familiar with some work that the FDA has done on data provenance when it comes to some of the data submissions for drugs and other applications.

So, we did our work in one month, so we started the Task Force at the beginning of January, we finalized our recommendations last Friday and we gave the briefing to the Standards Committee this past Tuesday, well, yesterday.

You know at the highest level I would say that our comments reflected that we thought it would be beneficial to the industry to have sort of a smaller scope of the use case and something that would be near-term, doable and impactful.

And we also advised the initiative to, as its next step from the use case, to go back and once it narrowed the scope of the use case to generate a core set of requirements for data provenance and they could use as an example a core set that had been defined by the FDA. I think in that case that core set of requirements is for research data.

We also recommended that they take a look at separation of communications and systems requirements and that we recommended that they take a further look at the impact of the change of data on provenance data. So, we know that we can track the source of the data, we need to define that term and what that data would look like, but the source of the data and where it goes, but we want to understand what it means when the data is changed along the way, how do you categorize those things, what are the impacts of them both in the clinical side and also as far as the trust decision with regard to use of the data.

So, our briefing slides are available, I think they're probably already posted, but the work...the next step will be that since the Standards Committee approved the recommendations that we provided, with one small addition from one of the Standards Committee members, that will go in a letter back to ONC as a recommendation for this S&I initiative on data provenance. So, they will have the recommendations and hopefully act on them to move the project forward. All of this is available on the FACA site, if it isn't there yet it will be there soon and then my understanding of the data provenance initiative is that they have completed the use case, they have not yet started the stage where they identify and evaluate standards, and they have not started writing the technical specifications.

So, it is at a good point in their process where they can go back and re-scope the use case, create a core set of requirements and then move onto standards evaluation and harmonization, and creation of the technical specification.

So, the Standards Committee also commented, I think, that this process of creating a very short-term Task Force to answer a very narrowly focused question is something that they were trying as a new strategy and they commented that they thought it had worked well, you know, we got a very tightly scoped question from...and a few sub-questions from ONC and we stuck to those and we each took a look at it and gave our recommendations and turned it back in. I think that we will see them using this mechanism again.

So, the Workgroups will continue and they will work on sort of long-term work plans and then when there is a question that might require some folks from different Workgroups or with outside expertise and we have a narrowly focused question, a narrowly scoped question they may form other Task Forces as well.

So, it was...you know, a unique and interesting experience, it was a lot of work but I think just, you know, keeping it focused on the specific input that's needed to move the project forward was a good way to do it and I appreciated being involved.

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

Yeah, and it was a lot...several people from the Standards Committee commented about how well that had worked that, you know, it was a very tight...you know, tightly scoped question, they got an answer quickly and were off and running. So, yeah, I agree with Lisa I think that we're likely to see more and more of that model being used.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Could we distribute those materials to this group? I know they're posted, but since I'm...

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

Oh, sure.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Have them distributed.

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

Yeah, Julie, do you think you can...once we finalize that one little piece can you send it to this group as well?

Julie Anne 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

Sure, I'll make a note of that right now, I can do that.

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

Yeah...

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

If you have any questions feel free to reach out to me.

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

I think you did a great job, thank you.

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

Thank you, Dixie.

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

All right, if we don't have any more comments then I think that, you know, we can open the line for public comment. Is that okay with everybody? Okay, let's do that Julie.

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 telephone 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 at this time.

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

Okay, well, thank you all very much for dialing in and I'm really pleased we were able to wrap up these recommendations. Thank you.

Julie Anne 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

Thank you.

M

Thanks, Dixie, bye-bye.

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

Thanks, everyone.

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

Bye-bye.