



**HIT Standards Committee
Transport and Security Standards Workgroup
Final Transcript
November 19, 2014**

Presentation

Operator

All lines 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 Standards, Transport and Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Dixie Baker?

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

I'm here.

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

Hi, Dixie. Lisa Gallagher?

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

Here.

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

Hi, Lisa.

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

Hi.

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

Aaron Miri?

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

Here.

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

Hi, Aaron.

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

Hello.

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

Brian Freedman?

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

Here.

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

Hi, Brian.

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

Hi.

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

Jason Taule?

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

Here.

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

Hi, Jason.

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? 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. Lee 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. Paul Clip? Peter Kaufman? Scott Rea?

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

G-Day, I'm on.

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

Hi, Scott. Sharon Terry? And Steven Lane?

Steven Lane, MD, MPH, FAFAP – 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? And Mazen I think you're on the line as well or you're on the line? Maybe not?

Kris Miller, LL.M, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

Hi, Michelle, this is Kris.

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

Hi.

Kris Miller, LL.M, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

This is Kris at MITRE we're covering for Julie today.

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

Okay, hi, Kris.

Mazen Yacoub, MBA – Healthcare Management Consultant

Michelle, hi, Mazen is on, I'm sorry I was muted.

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

Oh, that's okay. And I will now turn it back to Dixie and Lisa.

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

Okay, thank you, Michelle, and thank you all for dialing in today we really appreciate it. We know how busy everybody is and we appreciate you're giving us some of your time as well as your expertise. Today we're going to focus on the recommendations for identity management.

We're going to update or kind of remind people of what the Privacy and Security Tiger Team of the Policy Committee has recommended in terms of policy which of course establishes the context for our technology recommendations.

We'll speak a little bit about what really is a good recommendation. I know some of you are new to this Workgroup and new to FACA Workgroups perhaps so we do want to remind people that how we really need to frame our recommendations.

And then Lisa and myself, and the ONC team have come up with an initial at least starting point for some recommendations that we would like to...for today use them primarily to stimulate conversation about what we want to say to the Standards Committee when we present our recommendations next month at the December Standards Committee meeting. Lisa, would you like to add anything further to that?

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

No, thank you Dixie, I think you gave a great intro and I look forward to talking through the recommendations.

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

Good, good. I would also want to add, although it's not on the agenda, but for those of you who may have called in, dialed into the Health Information Technology Standards Committee meeting yesterday they mentioned that they were kind of changing how they were working with their Workgroups and they were going to launch some task teams and in that presentation they also said that those Workgroups that already had the work plan in place would proceed.

So, I just wanted to assure all of you that the work plan that we reviewed at our last Security Workgroup meeting is still active and that's the direction we're marching, and actually the ONC was pleased that we have made as much progress as we have and that we have our work plan in place so we're privileged to be moving forward on it. So, with that can we go into the next slide, please.

This framing is a reminder of some of the things that the Privacy and Security Tiger Team of the Policy Committee have recommended. I know that Kris and his team have distributed to you the formal recommendations that were submitted but we want today to just summarize them just to give a context of what we're recommending. Next slide.

The Tiger Team has made recommendations several times in the...beginning in September of 2012, have made a number of recommendations around identity management both for providers and for individuals as well. One of the recommendations that they made in September 2012 was to move toward multifactor authentication and this is NIST Level of Assurance 3 for remote access of protected health information.

As most of you probably know the NIST special publication 800-63 defined a number of I think four Level of Assurance, or LoA, each of those LoAs was a package that covered identity proofing to give somebody an account, authentication to authenticate their identity once they have an account and how the secrets used for identification or are used for authentication are protected.

The NIST, and Peter can provide better update on this than I can probably, but the NIST has been updating that 800-63 and Peter Kaufman, one of our members, has been involved with NIST in that effort in the past. Also, Paul Grassi talked about the current effort to update the 800-63.

So, the LoAs are, according to Paul Grassi last week, NIST is really moving away from the LoAs toward more modular ways of defining Level of Assurance. Peter would you like to say anything more about that or did he join? Is Peter on the line? Okay, he's not on the line, but he has been involved in that 800-63 update.

Another recommendation was to continue to identity proof providers in compliance with HIPAA so they concluded, and I was on the Tiger Team at the time when we discussed all this, and we concluded that there were plenty of mechanisms already in place requiring identity proofing of providers that we really didn't need to add anything more than what HIPAA already says.

And for several years since the NIST or NSTIC, the National Strategy for Trusted Identities in Cyberspace Initiative, was launched our Security Workgroup has been advised to be informed by and to keep abreast of, and to make our recommendations so that they are aligned with the NSTIC Initiative. Next slide, please.

In 2013 the Tiger Team made additional recommendations that ONC should define best practices for patient and consumer identity proofing and authentication for accessing patient portals, how an individual organization...we decided there really shouldn't be...we shouldn't recommend a specific policy change around that but that the ONC should really help providers understand the importance of identity proofing of patients and patient representatives when they give them access to a patient portal.

Similarly, they recommended that the ONC should define best practices for enabling the view, download and transmit functions that are included in Stage 2 of Meaningful Use and the 2014 certification specification whether it be for the patient themselves or for their representatives.

And again, they reinforced the idea of keeping engaged with the NSTIC initiative because that initiative will influence identity proofing, authentication, both identity proofing and authentication as well as the use of third-party credentials. Next slide, please.

So, to recap what we've heard so far, we've heard about OpenID Connect and OAuth 2.0 which actually combines the two together. OpenID Connect is the standard for single sign-on and to use a third-party...and combined with OAuth 2 is used for using third-party authentication and authorization to get authenticated and authorized to another application.

There are two profiles out there that we have talked about specifically, one being the Blue Button Plus which uses...implements OAuth 2 for the Blue Button Plus pull. For the push, where the provider pushes data to the individual it uses the Direct protocol and Blue Button Plus pull where a user or a user App might be able to query an EHR and actually pull data from the EHR, uses OAuth 2.

And the User Managed Access or UMA we had a presentation by Eve Maler about that...that's a profile of OAuth 2 that enables individuals to manage their own authorizations.

We heard about Trustmarks which is a way to componentize Levels of Assurance which is the direction that the NIST is now taking 800-63 and most recently we heard an update on what NIST is doing around identity management. Lisa, did you want to add anything here?

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

I think you covered it pretty well Dixie, I just wanted to remind I think that we, on our Workgroup, the recommendations from the Policy Committee's Tiger Team included recommendations around patient access and the scope of our work has included only the access for providers to EHRs.

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

Good, very, very good point. So, our discussion today does not include authenticating or identity proofing patients but rather really focuses on providers.

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

Right.

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

Next slide, please. A Federal Advisory Committee or FACA, which is Federal Advisory Committee Act, is a group of people from the private sector who advise the government and a FACA never really makes law or requires anything but rather makes recommendations that the ONC do something.

So, any recommendations that we make should say "we recommend the ONC consider" or "we recommend that the ONC continue to" or "support" which means that they would...like we've made recommendations that they "support pilots" or "further development of" those kind of things. But they're always framed in terms of recommending that ONC do something.

They offer guidance on what is needed, for example, in some instances the...in fact the Policy Committee is particularly fond of saying, they should use whatever levers are available, you know, there may be many ways that the government...many ways that the government can motivate people to do things, you know, the stimulus package and the whole HITECH Act was a perfect example of that.

But we really shouldn't make a recommend that says, ONC should pass a new regulation that says whatever, but rather we might mention that, you know, that they use available levers to incent or to regulate, or to, you know, to establish certification criteria around but not specifically tell them how.

Our recommendations should be more about what needs to be done and why than exactly how ONC should go about dealing with it, because they have experts that know exactly...all the law around how to really use the levers that are available to an organization like the ONC.

And right now we need to remain aware that anything that we recommend should be very much well aligned with the interoperability roadmap that is being developed by the ONC the initial version which was briefed to the Standards Committee at the October meeting of the Standards Committee.

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

Dixie, this is Lisa, may I add something?

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

Yes?

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

So, this may go without saying, but what we can also recommend that we on the Workgroup or the Standards Committee do something. So, if we recommend that we continue our work in a certain area or that another Workgroup, or other group of SMEs on our committee do further work in an area we can certainly say that as well.

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

Yeah, very good point, very good point. Okay, next slide, please. Okay, these are our draft recommendations and as I said earlier they really are intended to motivate and stimulate discussion in our Workgroup today. We are expected to present recommendations around identity management for providers at the December Standards Committee meeting.

So, the first one is really...follows onto a White House Executive Order that came out around multifactor authentication, it came out what in, let's see October, October 17th and there is a foot note there that has the link to it.

But the White House stepped forward and said that whenever anybody...whenever a system is authenticating an individual to access personally identifiable information that multifactor...multiple factors should be used in that authentication. So, our first recommendation is that multifactor authentication should be used to access PHI.

The second one is to support NIST in the revamping of 800-63 and the third, I'm just going over it briefly now and then we'll go back and address each one individually, the third is action related to the data segmentation for privacy specification it's an HL7, I think it's a draft standard for trial use at this point, I think. And the last one is to continue to track the development and piloting of UMA and the UMA profile.

Okay, do we have...regarding the first recommendation, multifactor authentication for access to protected health information, do we have...now do we have any discussion around this? And this is for provider authentication. Now, initially the Tiger Team made a recommendation that multifactor authentication should be used for remote access to PHI.

And at one of the Standards Committee meetings where Lisa and I presented recommendations the members pointed out that in today's environment it's really difficult to define what "remote access" is. So, if you have thoughts about how this might be constrained or whether it should be constrained I'd certainly be interested in your thoughts about that.

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

Well, this is Steven Lane and I'd like to comment in a couple of ways on this one. One is that I come from an organization, Sutter Health in Northern California, and we have required multifactor authentication for remote access to PHI for over 15 years and have gotten a lot of flak in our region because other organizations in our region do not require that they let people in with just an ID and a password, but it's certainly a position that we have held and maintained and one that I very much support as a national recommendation.

When you go beyond discussing remote access and I appreciate the challenge of defining what that is, you know, when you're talking about clinicians working within the four walls of an organization and potentially logging on and off of PHI containing systems hundreds of times a day having to use multifactor authentication, you know, depending on the available technology, may present an insurmountable barrier.

Now, I mean, if I had an RFID chip, you know, in my forearm and it knew that, you know, when I walked up to the computer that would be fine. I think having, you know, introducing a fingerprint reader, you know, every time you log on and off that would be a challenge. Certainly, any kind of a token, you know, that you would have to access and, you know, copy numbers off of or whatnot would be very challenging.

So, I think, it's a big step to go from multifactor authentication for remote access to in-organization access and one that I'm very interested in hearing what others think about.

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

And how do you...how did you define remote access? Of course it was a little easier 15 years ago, but how do you define it today?

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

Exactly, yeah it really was easier 15 years ago. I mean, today we use mobile devices, you know, that obviously function both inside and outside of our buildings but there I believe, my understanding is that the device itself provides the second factor for that authentication. So, I think that works pretty well but when people are logging in, you know, from home or from, you know, an Internet café or whatnot then then, you know, we certainly do require a token.

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

That's interesting. So, when you authenticate from a Sutter device the server knows that that's a Sutter device, it authenticates that that's a Sutter device?

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

Well, we're moving in that direction. When I authenticate from a mobile device, you know, like an iPhone or something like that, the device itself has been registered with the application so that the device serves as that second token. So, I know who I am and the device is the token that then justifies the access to the system.

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

That's interesting.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
So, one of the...

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

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
Yeah, this is Scott...

M
Yeah this is...

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
Oops, sorry.

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

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
So, one of the things I was going to say is it's interesting that if it's specifically multifactor authentication or whether it's merely a Level 3 on the NIST scale for authentication because you can reach Level 3 with some technologies without having multifactor authentication although multifactor is the typical way of achieving that.

And it's interesting that if you specify multifactor authentication you start to run into some of the issues that have just been enumerated which becomes a challenge for users especially when they're, you know, in their normal place of work and working internally it becomes a barrier, a usage barrier.

But if it's really to specify Level 3, which can be achieved by multifactor authentication but can also be achieved by some other ways which are a little bit more user friendly and so that was my question, is it specifically multifactor authentication we're after or is it more Level 3 under the NIST 800-63 standard?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Well, I thought Level 3 was multifactor now I don't know of any other way that you can authenticate at LoA without multifactor.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert
LoA 3 can also be facilitated with a medium assurance software certificate PKI.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Oh, in that case that though that would be considered the second factor.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society
Well, and I think I want to add Dixie that...

M
Okay, so you...

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

I'm sorry, this is Lisa, Scott, also, you know, I think we probably need to discuss whether we want to in our recommendations specify specific LoA or given the potential path that NIST is going away from that maybe just talk about the components like multifactor in our recommendations. So, I think that's the discussion that Dixie and I had and want to have here.

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

Yeah, but for the...

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

Yes.

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

For this conversation, you know, I think he's just referring to LoA 3, but yeah I agree with Lisa that we really need to keep aligned that's recommendation number two, but, so let's just talk about multifactor.

I think when you use a software certificate plus a password then you have that, just as Steven described at Sutter they use the device and the individual, I think you can use a software certificate as one of the factors. I wish that Peter our 800-63 expert were here but that's my understanding. Does anybody else know?

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

So, Dixie, this is Jason Taule, it depends on how the person got their credential. So, it really goes back to registration and identity proofing. If it's a source of record than that second thing can be a second factor if not then it's a second instance of the same factor, right, it's no longer what you have its two instances of what you know.

I know that there are some companies in the financial space that talk about two-step authentication that's not multifactor that's two instances of the same single factor. Right, so, from a...

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

Well, that's...

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

If I could just elaborate a little bit, what I think the Policy Committee was after was that we establish strong authentication meaning that the person on the other end cannot later repudiate that they gained access to the individual's PHI.

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

Right.

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

So, if we're focusing on the standard for making that happen than we need to talk about, you know, should it be multifactor and then whether some of the things that are within 800-63 should be adopted.

I don't think it's the same solution for providers as it is for patients because providers have the context of within the healthcare setting whereas the previous person mentioned it would be very much of an encumbrance to continue to make them do something but for patients the frequency of access to their data is relatively minor compared to a provider and everything that a patient is doing to access it is always remote. So, I think we want to make that distinction. And then the last point, it completely slipped my mind here, it will come back to me.

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

Well, how do we...we can't...I don't think we can toss around the term remote any more than anybody else. I think that we...if we want to make a recommendation that limits two-factor authentication to "remote access" we need to define what that means.

Luckily, we can define it in terms of technology instead of policy which I think makes it a little easier, a little easier anyway. But, I do think that we need to constrain it I know, in fact I know that, because if Lisa and I once again, you know, appeared before the Standards Committee and said "we recommend two-factor authentication for remote access" we'd get the same reaction "how do you define remote access?" So, I think if we want to make that recommendation it's incumbent upon us to define what we mean by remote access.

The other point I'd like to add to this though is that, you know, the JASON Report, Task Force, and the Nationwide Health Information Network Power Team both recommended, you know, the use of OpenID Connect to authenticate providers and OpenID Connect of course allows one to reuse, you know, it's a single sign-on specification, it allows one to reuse an authenticated identity and when you do that it becomes even more important that the initial authentication was strong, you know, you don't want a strong...you don't want a very weak authentication to then become a single sign-on token that gets sent all over the place and gets you access to everything there is to access.

So, I think there are definitely other factors in today's environment that you really have to consider when you consider the certification of authentication.

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

Dixie, this is Lee Jones, if I could make just a couple of comments?

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

Yeah, hi, Lee.

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

Hi.

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

Glad you could join us.

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

Sure, so, I guess one, I totally agree or maybe said another way, I think that this idea of remote versus non-remote is going to be very, very difficult to define because even in our, you know, context that I work in with a lot of these value-based payment paradigms where there are lots of care coordination among disparate organizations that have come together in a federated way, you know, under like a health home or an ACO, etcetera, we're already running into tricky definitions of the covered entity and what is really local and what is in it, you know, all of that.

So, I probably would shy away from trying to qualify it at least in that way in terms of remote versus non-remote, but I would say that I would also support, as I think some of the previous presentations that we've seen in this meeting have, I think, at least in spirit, talked about the segmentation of information or the determination from a source about the level of access of information rather than have a blanket two-factor authentication hurdle for access because I think that lots of these systems have different levels of aggregation of PHI and/or ways to obfuscate things, etcetera, and/or expose stuff and there are already complicated consent rules and other things that people are enforcing.

And I think that the confluence of all those things for a software developer who is providing access to PHI really, you know, gets convoluted and not implementing consistently and probably is more of a usage barrier than is necessary but I'd like to see people who make systems that may not have that bar of two-factor authentication as maybe defined here whether you allow certificates as one factor or not to still be able to grant access to, you know, other...to data that the community has deemed as...that having already been checked through some sort of, you know, policy or mechanism or however they choose to solve those issues. So, I just am afraid of such a broad brush and the implications on the software that has to protect this data.

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

This is Brian Freedman.

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

Yes?

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

So, really two things I guess, one I've worked with, in the past with Navy Medicine, they have 60,000+ users, they have hospitals all around the globe and they've implemented single sign-on, two-factor authentication using basically a SMART card or, you know, the Common Access Card is what DoD calls it, it's been very successful, it's been going on for several years, you know, if you need access to, you know, any information you have to login initially with, you know, two-factor authentication remote, in the hospital.

And then there are some interesting technologies that actually make certain things easier where you could, you know, with the SMART card you could...as you walk from room to room and you put your SMART card in it, you know, automatically can bring your session up, but without getting too far in the weeds of that, I mean, that's just one example of a successful implementation of two-factor authentication, you know, which actually has a side results of protecting protected health information.

And then I think on the other point is that just from the security risk assessments that we do, especially around HIPAA, especially in private, you know, independent practices and that kind of stuff it's just rampant the amount of sharing of passwords, you know, between a doctor's nurse and then there becomes some kind of issue where a nurse maybe prescribed something that she shouldn't have and, you know, but under the doctor's name and, you know, everyone like has their arms up in the air, you know, of who did what, you know, so something definitely needs to happen because that's probably unfortunately more the norm that I've seen, you know, than is probably out there and I'm not saying every organization is like that but there are many organizations out there that have that same particular issue.

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

This is Peter Kaufman, I'd like to speak to that also.

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

Oh, thank you for joining us we missed you Peter.

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

Yeah, I know, I'm sorry I was in another meeting, sorry I got here so late and of course I missed the bulk of the meeting, but I think that this is going to be the biggest problem also the doctor's sharing passwords and tokens.

DEA has said, in private meetings, that they're looking for a test case and I think that will scare the beejebees out of a lot of healthcare practitioners but I'm not sure it will stop them from doing it. The DEA is going to find somebody who had somebody else write a prescription with their token, you know, two-factor authentication and they're going to go after them.

I have to tell you I went into a doctor's office a number of years ago that was using our ePrescribing and his staff person, before we had a provider agent role, just was entering his password to send the scripts we have a separate password for sending scripts and I said to him, in front of her "that's like you gave her a pad of signed prescriptions for her to fill out whatever she wanted on" and I'm not making this up, she opened the draw and pulled out a prescription pad where every prescription was signed by the doctor and the prescriptions were blank.

Doctor's don't really...they're thinking about workflow and they're trying to get this out and I think that this is going to be an issue where people are not going to take it seriously enough that their token is their token. Biometrics might work a little better but tokens are going to be an issue and passwords too.

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

And I'll just echo that this is Steven Lane, I mean, having lived in the clinical environment for decades we certainly have heard of people, you know, not only giving out passwords but giving out tokens to others, it certainly never happens in my organization but we know it happens out there.

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

Yeah and this...

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

Well, I think it's hard to prevent even with biometrics because if somebody...unless you combine that with...well, even with biometrics because once the person has authenticated themselves if they then allow anybody to act within their session it's the same, you know, it's exactly...it's identical to sharing your password there is really no real difference in effect, yeah.

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

Yeah and this is Lee Jones again and I guess just to...you know, the confluent...in New York for example where there is a strong Medicaid Health Home Program and hospital systems and other providers that are part of multiple health homes which may or may not use the same technology, the confluence of all of the third or the second factors that you have to keep track of in order to do a similar thing where you may or may not realize that you're a part of this health home for this classification and that health home and that classification, this is my journal system, this is my RHIO, this is my HIE whatever it is all of those different things not being done in a coordinated way just puts a heavy burden I think contributor that, you know, just get it done kind of attitude as opposed to a physician trying to track it which way they need to authenticate.

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

So, what's the solution? It sounds like it's not even a matter of two-factor or one-factor people are sharing their authenticated session.

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

So, Dixie, this is Jason again, I think the recommendations that we can make can parse this into multiple objectives because I think the first objective is about having patient confidence that the people who are seeing their data are the ones who are authorized to see it.

As a second objective making sure we've got strong authentication that it was that individual provider versus another provider that's a secondary objective. They can both be supported by multifactor but that doesn't necessarily mean we have to...you know, we can eat this whale one bite at a time, right?

So, I think, we can talk about multifactor solutions that help make sure that it's only the people that should see it that are seeing it not necessarily tying it back to an individual provider so that it's not somebody else, it's not the hacker getting into the system that's hosting my EHR so that the patients are concerned that their data is exposed when their doctor goes to get it.

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

Well patients learn that anybody sees their PHI, you know, that they don't know about, you know, they know that the internal, you know, the internal hack...they don't call them hacking, misuse of access to systems is a problem I mean that comes up all the time, you know, within...

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

Right, right.

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

Organizations.

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

Right, but what I was saying is that's happening today and we may be able to make improvements on that but the concern is going forward in order to facilitate exchange across a broader ecosystem we need to make sure that we don't make the problem worse by adopting the solution that allows anyone who is not a healthcare provider to get into that sensitive data.

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

I see, well, you know, going back to what Steven said about what they do at Sutter, you know, they have multifactor for remote access but they consider the device itself as one factor within an organization you could do the same thing, right, if they're logging in from a device that's known to be within the organization can that be one factor?

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

Well, but...

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

Sure if its white listed, this is Aaron Miri at Children's, this is what we do. We actually use NAC to be able to control the devices that we know we own and so based on MAC address even though that can be spoofed and a certificate that we do put on every device which we refresh on a periodic basis those devices suddenly become credible devices. So, you still have to have a username password to get into the App but the actual functional device actions as also a factor.

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

Is...

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

That makes a lot of sense.

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

Mindful that we have government systems as well as commercial systems that won't hunt in the government space because the second factor has to be on a platform apart from the one used to authenticate.

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

Yeah, but we're not saying that...we're not trying to establish a common policy that's enacted every place we're trying to recommend the, you know, what systems need to support, you know, and their certification.

So, what we would do is we would recommend that a certified system be able to pass a, you know, some kind of...whether it be a MAC address or storage certificate, you know, basically that any certified EHR technology require multifactor authentication for any access to PHI but that an identifier that identifies the device they're logging into can serve as one of the factors.

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

Dixie, I want to apologize for coming on late but I'm missing an important part of this conversation and I just want to make sure I have it straight.

Are we discussing that the certified systems will require any users as accessing PHI to use a two-factor authentication or that the certified systems have the capability of requiring any user to use the two-factor authentication to access PHI and let the market decide whether they're going to use it or not?

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

Yeah, that's a really good question, it's "B" you know we really don't...the Policy Committee does policy and the Standards Committee does standards for certification.

So, when we recommend...when we have a standard the standard for certification would all...it would never say, every provider must authentication herself twice before she can access PHI that's policy.

What it would say is that any certified EHR technology must have the capability to require two-factors in order to access PHI.

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

Perfect, thanks.

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

Dixie, this is Aaron, would we also be able to somehow recommend perhaps following other standards such as FIPS 140-2 or something else especially that the healthcare market is already accepting as policy so that we go along with other accepted policies? I would just worry about two different potentially conflicting, you know, mindsets approaching two-factor.

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

FIPS 140-2?

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

Yes, Ma'am.

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

What is...that's not...let's see its 140-3 NXA is the encryption one, right? So, what's 140-2?

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

Yeah, I mean, it's about the...it's basically the physical device cryptology it's the standard basically for all the FDA narcotic dispensing for two-factor and it's what we're all having to do, FIPS 140-2, it's about two-factor authentication for dispensing of narcotic medicines, Class 2 drugs those kinds of things.

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

I see, okay, thank you.

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

But we don't want to specify specifically 140-2 because 140-2 limits it to two dimension and some of the newer three dimensional biometric devices are not capable of doing 140-2 but are capable of being equivalently safe so you have to be careful about that.

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

Right, I’m using that as an example just some standard that’s in the market that we would follow kind of in that same realm. So, we’re sticking with...

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

That’s the ideal, if there exists a standard that we could recommend to be incorporated in the certification criteria that’s the ideal, it’s much more...it’s much preferred to cite an existing standard than it is to just cite a functional requirement. So, actually that’s what we should be striving toward is something like that.

If you know of, you know...now 800-63 is really a special publication so it isn’t a standard as much as a FIPS, you know, or an IETF, or a, you know, HL7, but if you do know of standards that would be citable for two-factor authentication that we could use as the authentication component of this that would be good. I don’t know of any that, you know, that we, you know, that are like FIPS 140-2 it sounds like but are not specific to dispensing of narcotics.

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

Well, the DEA description that they have in the interim final rule, which includes mentioning 140-2, was not poorly done, it was pretty good.

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

Interim final rule of what, FDA?

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

For controlled drug ePrescribing.

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

Oh, I see.

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

Yeah, it’s a big deal for hospitals right now. I mean, it’s a big, big deal for providers.

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

So, what are you recommending both of you? Are you recommending that this be something we consider?

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

I think that or something similar, I’m not saying that be it, but I do know that as I speak with my peers in the market that we’re all looking at solutions that gravitate towards this and a lot of solutions are moving their products towards being able to be this specific, but, I mean, it’s just an option on the table.

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

Yeah and I’m suggesting that we probably include that as an option in our specification but we may want to look at the language of the DEA’s EPCS interim final rule to see how they worded it since they, you know, went through this a couple of years ago and although the technology has changed I think that they were planning ahead as best they could for technology.

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

And I'll just add the clinician's perspective since we are in fact live on EPCS and have been for a few months, it's really been, you know, as I mentioned earlier the need to use two-factor authentication in the clinical setting is really a big change and while our providers love the fact that they can now electronically prescribe these medications and that they don't have to, you know, hand write paper prescriptions and in parallel enter the data into their electronic medical record it is a challenge and we've, you know, distributed tokens, we've done biometric fingerprint readers and I think the jury is still out as to how usable these are.

In our organization with a few months of experience we still don't have even 50% of our prescriptions for controlled substances going electronically. So, I think, again, introducing the requirement for two-factor authentication, you know, if it's not workstation based is really a challenge in the clinical setting.

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

At the risk of talking too much on this but we're getting into an area that I've got a fair amount of experience and it's so rare on this committee that I know anything that everybody else doesn't already know, we did a pilot project in Western Massachusetts with physician offices and now we're nationwide with, you know, our controlled drug ePrescribing, we're sending over half the controlled drug ePrescriptions and we've learned a lot about scalability.

If you're in a hospital or health system you can do biometrics, you can do crypto keys, you can do all sorts of things because you have control over drivers and devices. If you're dealing with individual physician offices, which there are still an awful lot of offices around the country, then you don't have the scalability capabilities of having somebody there in the office to fix it when they get a new computer and the drivers don't work under the new operating system.

So, we learned to use something that didn't require a driver which makes it much more simplistic and a harder workflow for the user. So, it's going to be even more difficult than what was just described because in a hospital you have the option of doing things like biometrics, in a doctor's office you don't. And so until the technology gets advanced further it's still going to be difficult to doctor's pulling out, you know, basically the one-time password device where they have to copy the six numbers over.

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

Well, but we do use fingerprint readers in the office just to be clear.

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

Yeah.

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

But in most doctors' offices they can't, you know, whoever their vendor is isn't getting to the office to put the fingerprint readers in, in a scalable way.

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

Yeah, I mean, for us...

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

That's an issue.

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

They are \$100.00 USB devices that you just plug in.

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

It's not the matter of cost and they're even cheaper than \$100.00. The matter is the drivers, their computer dies they get a new computer, the driver doesn't work with it and, you know, driverless technology is coming but it's still a consideration that because of scalability the devices being used are more of a workflow interruptive device and could be if it was a crypto key or a fingerprint or a tap and go card which for some reason nobody is making a tap and go card that's FIPS 2 compliant.

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

So, do we want...with respect to our first recommendation here, as we said earlier the certification criterion needs to say something like the certified EHR technology must be capable of...must have the capability to require two-factor authentication, you know, two-factors be presented before the individual is authenticated and suggest wording that maybe Peter you or Aaron could extract from that NPRM for us to use with respect to number one?

In other words we would recommend that there be certification criterion which doesn't require anybody to use it, as we've pointed out earlier, it just requires that the technology be capable of it, but now is 140-2 is that technical language in there or is that more policy language?

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

I'd need to look through whole thing Dixie to be very honest with you. I think I know the answer but I want to be specific. It seems to be more policy but there is some technical, but it is more policy-driven. But, let me validate.

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

Okay, is that what we want to try to hone in on? Maybe if we got you guys to give us the wording, look up that wording in the NPRM and maybe we could combine it in a recommendation that certified EHR technology be at least capable of supporting two-factor authentication.

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

Okay, we can do that.

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

Yes.

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

Okay.

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

Yeah Lee Jones, I support that also.

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

I'm very much in favor of what you just said.

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

Lee, were you trying to say something there?

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

Yeah, I was just saying, I'm much more supportive with the "capability of" language.

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

Okay, so our first recommendation will say that we recommend that certified EHR technology be capable of supporting...capable of requiring two-factors in order to authenticate that's our recommendation briefly. And if we have...if we can get...if we decide between Peter and Aaron, maybe I'll just have you guys look at that and if we can find some wording in the NPRM that we should consider maybe you could present it back to this group at our next discussion.

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

Sure.

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

Okay, thank you. Okay, let's move to the second one, this is to support the NIST effort to revamp the NIST SP 800-63 and to closely follow the move from LoA to componentize trust, and to recommend appropriate identity proofing for query-based access.

As I said earlier, before Peter joined us, Peter Kaufman has been working with NIST on the latest update of 800-63 and he has agreed to track the continuing work on that standard for us and to help us keep abreast of what's happening there. So, Peter could you tell us...I know that there has been an update to 800-63 I think its 800-63-2 or something that you were involved with, would you brief us on the latest change?

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

The latest that I am aware of, because I haven't talked with anybody at NIST for a year, but the latest is 800-63-2 which was an update to include a couple of factors for identity proofing, one of them was the ability for a hospital or a healthcare institution to identity proof their users.

The thought behind this was that for a physician or practitioner, a healthcare practitioner, to be certified in the medical staff of an institution usually they're going through higher than a Level 4 level of authentication. They have to present themselves in person, they have to provide information including previous medical licenses and current medical licenses, diplomas and even their transcripts from medical school, it usually involves an interview, it's a very intense process at most hospitals and is required for hospitals to get money from Medicare.

So, they put in, you know, the wording that if the hospital was a Medicare certified institution or the hospital healthcare system was Medicare certified that the medical staff office could certify the providers directly without requiring a separate identity proofing.

The other thing that they put in was the ability...and this is something that we didn't ask for but we're delighted to see, the ability to certify an address by contacting the identity profee through something that was billed to their home. So, if they have a cell phone that's billed to their home phone or are calling the home phone they can either call and read out a four digit number or they could send a text message and the person would then put that into the application and complete their identity proofing.

What was required prior to that for a Level 3 or 4, other than in person identity proofing, but if it was being done on-line, it was required to mail a letter to their home address which they would then have to have the code on the letter and enter the code in the computer, so it would take at least a day even if you were FedExing and be relatively expensive and this allowed if the person did have a phone that was using their home address, as opposed to a business address, that they could be contacted via that device to complete the identity proofing for on-line identity proofing.

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

So, the phone one is if they have a phone and they get the bill at a particular address then what do they have to do after that?

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

The identity proofing system will have that phone number through its various Internet activities, either Verizon or Experian will have that phone number, which is billed to the home address, and will send a text message or make a phone call to that number to identity proof.

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

I see.

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

A lot of systems are doing this now in fact Hopkins has just started doing this if you want to access the Epic program outside of the hospital they're going to...if you're using a new device, they're going to call your cell phone or send a text message to your cell phone and you have to put that number in to verify that you're the person on that device. So, it's a form of a two-factor authentication that is a little lighter than actually getting a crypto key or a...

M

Right, it's what the banks are doing and others.

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

So, Dixie, this is Lisa.

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

Yes?

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

So, that was a really nice summary from Peter on the update that were in the dash two version but I think here we're recommending also that we continue to look at what NIST plans to look at in that document for FY14 and 15. And if you don't mind, I'd like to summarize those points that...

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

Sure.

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

Actually gave us. So, the question that they're posing to themselves is what if NIST just measured authentication performance or strength or usability thinking in terms of componentization of trust and assurance elements and supporting the assembly of vectors of trust and that looks like similar to what we saw in the briefing on Trustmarks from GTRI.

And then posing the question, if we could do that could we get rid of level of assurance and update the document to specify trust and assurance elements in terms of components and then vectors of, you know, combined into vectors of trust.

They also said that they're considering a private sector companion to 800-63 and wanted to know also what else could we do to sort of update the document and facilitate its applicability as we go forward with the development of technology.

So, I think that's why we have this recommendation here under the first bullet which is to continue to dialogue with NIST to be involved, to give them the perspective from healthcare, etcetera, as they consider those elements for the next year or two.

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

Yeah, to make sure that our, yeah, that our...the healthcare industry's needs are reflected in that revamp and I think between what this second recommendation is really...between the ONC's involvement with NIST in that revamp of 800-63, which already is happening, right, Kris, you're on the phone that's true, right? ONC is already working with them? Are you there?

Kris Miller, LL.M, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

I believe, yes, I believe that was the consensus from the messages that were exchanged yesterday, that's correct.

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

Yeah and between...so what the ONC is already doing and our being able to capitalize on Peter's activity independent of that, that we can really keep abreast of the changes and, you know, avoid making recommendations to the ONC that lock into an old version of that special publication. So, I think that's...I think that's the essence of that second recommendation right there.

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

Right.

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

Okay, why don't we move to the third one which is way harder. The data segmentation for privacy or DS4P is a profile that was developed by the S&I Framework of the Office of the National Coordinator and then handed over to HL7 and I believe it's a draft standard for trial use at this point.

But what DS4P does, and it's probably one of the most misunderstood works out there these days, there is one law that requires that not only...that applies not only limits who...well, number one, it requires separate...explicit authorization to share an individual's health information and that's Part 2, what's it, 21 CFR Part 2? There are twenty-five. It's a Part 2 data, which are behavioral health data.

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

It's 42 CFR.

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

Forty-two, 42 CFR Part 2, which is behavioral health data and it explicitly requires that an individual must give their authorization before their health information, their behavioral health information can be shared with another provider, so it doesn't come on the treatment, it doesn't come under the treatment payment and healthcare operations exception, it explicitly requires the individual's authorization and furthermore it requires the individual's authorization for the provider that receives the information to share it with anybody else. So, it severely...that law really requires the explicit segmentation of behavioral health data apart from other health information.

And so the DS4P profile is to enable one to electronically exchange behavioral health information such that it carries metadata that says it is Part 2 data and that the recipient can't further disclose it or even integrate it with their normal EHR, it has to be separately managed, separately segmented out.

So, I think, that right now the certification criteria do not include anything around data segmentation at all and so we thought perhaps we should recommend that DS4P be considered as a potential certification criteria to authorize access to behavioral data.

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

So...

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

Now, I think this is a tough one because in a lot of healthcare organizations they simply use separate systems for behavioral health Part 2 protected data.

So, I think that there...we may have some discussion around whether all EHR, certified EHR technology, needs this or of course with the modules now, you know, there is no...you know, the way they certify EHR technology now it's all modular, it's no complete EHR technology so that issue probably goes away.

I guess the question really is, should there be a certification criterion that addresses certifying EHR technology to support the DS4P profile?

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

So, Dixie, if I might, this is Jason Taule again, I know a little bit about this. We actually built the first system for SAMHSA under the OBHITA contract.

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

Yes.

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

One of the objectives was that there were some studies done that showed there were an awful lot of healthcare organizations that were actually not taking advantage of all the many benefits that electronic health information exchange offers because of this challenge, because most...up until now we basically gave consent on the record as a whole rather than individual elements and by having this system it allowed us to show respect for the patients not get ourselves in trouble relative to some of the more sensitive components of the record and yet share with providers the data that they needed to deliver other types of care apart from the substance abuse or mental health-related issues.

So, I would certainly endorse this, you know, if my involvement means I need to recuse myself because of my obvious position in favor of this...and yes this actually is out in trial now we're doing a number of different pilots actively under way and getting very, very favorable feedback.

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

And I'd also like to chime in, this is Steven Lane again, with the practicing physician's view I think one of the challenges with this, and we've struggled with this for a long, long time is that behavioral health data exists in many places in the chart so there are the notes from specific encounters with behavioral health professionals and then of course there are all the problems, medications, results, references to behavioral health-related information that exists throughout a patient's medical record ideally in every primary care visit, etcetera. So, I'm not familiar with the DS4P standard, I think it's appropriate to consider, but I think the devil really is in the details.

I would also just throw out there that there are other kinds of data in the medical chart that warrant specific attention and one area that I've been working on recently is adolescent data at particular types of information within an adolescence record that have special privacy considerations so as not to be shared with anyone other than...or specifically not to be shared with parents or guardians and I think...and I don't know if there is a standard developing around that but if so that perhaps also should be considered.

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

Sure, to respond to that point, this is Jason again, actually the way this is working is we're giving the consent options to the individual whose data we're talking about, they can parse it almost anyway we want and once the data map is in place it will allow an institution to customize it to whatever their purpose is. If they want to say, I want to share this record but not that one with this provider but not that one, all of that is in the consent to share system.

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

Right, but again...

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

Yeah, but that's not what...DS4P they're always very, very careful to make sure they're talking just about behavioral health data. And I'd like to respond to you Steven because I recall that when the Tiger Team discussed this, the DS4P, one of the things that really surprised a lot of us was the diversity of views on what Part 2 data were and just because a doctor, you know, if you tell the doctor that, you're family practice physician, that you have an alcohol abuse problem that is not Part 2 data. Part 2 data specifically refers to data that are protected under SAMHSA regulation.

So, just because somebody tells you something about, you know, that they have a drug abuse problem that is not...that doesn't make it Part 2 data and it's not applicable to the DS4P protections and the SAMHSA protections.

So, the doctors that are panicked that, you know, a patient told them about their drug abuse problem they need not be panicked because that's not considered...that doesn't fall under the Part 2, CFR Part 2.

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

And I agree with you Dixie, but I hear in many conversations people saying, well, we can't display these problems, we can't display these medications, we can't display, you know, that sort of thing and so I think people go beyond that when they think of this.

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

I know they do, I know, even one doctor that was on the Tiger Team said exactly that, exactly that and the person from SAMHSA that's who clarified that this is not really the intent. There is a lot of misunderstanding of what it's all about and there is a lot of misunderstanding about what DS4P is about as well.

So, and I think that this is probably the risk associated with making a recommendation around it is that there are so many people that think that every doctor has to segment out, you know, sensitive information which is not the case.

But fortunately, we aren't a policy organization, we're a technology organization, so all we would need to do is recommend that they add a certification criterion that certifies a system as having implemented DS4P that's basically what we would be recommending.

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

This is Brian, I agree, I work with Jonathan Coleman with S&I, he's on the S&I Framework and he's doing a lot of work with DS4P and I mean, if you put on your patient hat for a second, you know, it just makes...it makes a lot of sense. So, this should be something that should be pushed forward as a consideration.

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

The only question I would have is that, you know, we the Standards Committee has a number of...has developed a number of criteria for when...for judging when a standard is ready to become a national standard and they are more or less followed. But have there been implementations of DS4P besides Connect-a-Thons and pilots? Does anybody know?

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

This is Brian again, they've put forward, actually just recently, I think they presented it yesterday, you know, scenarios where this could be used and, you know, from my understanding though it's not in any like full scale production anywhere at this point though.

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

Is that the briefing that Jonathan gave at the Standards Committee meeting yesterday, Dixie? Because we had some feedback for him if you recall.

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

Oh, that was about the data access, DAF.

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

Oh, okay.

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

Data Access Framework I think.

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

No, he presented on the data segmentation privacy.

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

Yeah, he has before but did he...I don't think he talked about that yesterday, but I could have been zoned out. I think he talked primarily about DAF. But he has talked about data segmentation for privacy in the past.

I'm not a big fan of recommending, you know, for a national standard something that really isn't in production and it's not just me, the Standards Committee is very hesitant to support that. So, that would be a concern that I know that we would hear if we presented that recommendation. So, I don't...

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

I could get you some more information from him, you know, around that if, you know, what, you know, what information...where it has been, you know, tested or used, or done, etcetera.

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

Yeah, actually, as we have on this slide we are...that would be very useful Brian to respond to you, but later in our work plan we're going to specifically address DS4P. So, maybe...

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

Isn't this recommendation okay the way it is then? Because we are going to consider it and it is on our work plan. So, we'll be able to look into it more deeply and give a complete recommendation at the end of that task.

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

Actually, that's a good idea because if we briefed it now...if we just presented this as it is, consider, then when we get farther...when we actually get to the DS4P point, you know, we could benefit from feedback that we would receive from the Standards Committee when we present it next month. So, yeah, maybe that's what we should just do just leave it like it is a "consider" and then...

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

Yeah, Dixie, this is Aaron, I like that idea, I think that’s a great point.

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

Okay.

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

So, Dixie, this is Jason again, I’m going to...my only input is that whether it’s the DS4P as the standard I think the goal is to make sure that one of the certification criteria is that it address this issue. Right, that’s really what we’re about.

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

Yeah, I think that’s right and Dixie we’re going to have to look at this closely because there are multiple...there are several possible implementations in order to meet the requirement and so we have to really look at, you know, what’s the right thing to recommend.

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

At this point or when we get to that in the work plan.

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

When we get to it in the work plan.

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

Yeah, yeah I do understand that the whole behavioral health community would like there to be a certification of this capability in there.

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

Yes, but, you know, what standard we recommend and, you know, how that impacts the certification and the vendor’s products that’s something that we have to look at.

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

Yeah, yeah, I think that’s what we do...but Brian if you can find out if there have been implementations that would be useful in our planning for testimony that we receive around DS4P when we get to it in the work plan. So, that would be really useful to us, thank you.

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

Okay, thank you, I’ll take care of that.

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

I’ll make myself a note, okay. Okay, how are we doing for time here? It’s...

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

Yeah, I think we're good.

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

Okay, so should we go to the... and the last one is pretty non-committal as well which is to track the development and piloting of UMA, the UMA profile's OAuth 2 as a potential standard for consumer consent. As we were told...you know, UMA is a very...it's a new profile and it's being demonstrated in Connect-a-Thons and it's being piloted but it certainly isn't in broad use. So, I think what we were intending to do here is to just raise the Standards Committee's awareness of it as a potential solution for automating consent.

As we all know consent these days is usually implemented as a paper that somebody signs and it gets filed away but as we move forward we know that the ability to attach machine readable consent authorizations to data is going to be a policy requirement downstream and so I think that just making the Standards Committee aware that this exists is what we're trying to achieve there. Are there any other suggestions how we might improve that or make our point better or disagreement in making the point or any thoughts at all on that one?

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

This is Aaron, again, from a provider perspective I welcome it. To your point there are multiple consent forms that are always, you know, floating around for any kind of reg or whatever procedure anything. So, anything we can do I think the community will rally behind it.

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

I think so too, yeah. It's hard to get people...I do a lot of work around automated consent and it's hard to get people when you even use the term consent they automatically think of a piece of paper, you know, and how we can make it into a PDF and stuff it into a C-CDA or something...

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

That's...

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

I'm eagerly looking forward to the day when we can automate consent permissions. Okay, I have two, let's see, we have two follow-on, we'll be...Lisa and I, and the ONC team will be updating these recommendations and we just have two voluntary follow-ups is Peter and Aaron will look up the wording in the FIPS 140-2 NPRM.

And Brian will find out for us whether the DS4P is implemented and, you know, maybe even some recommendations, if it has been implemented, maybe some recommendations on people to talk to us about it that would be useful as well.

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

I looked up a lot of it during the meeting and it's showing a requirement for FIPS 140-2 security level 1, which is mentioned repeatedly through it but that's a very low level of security, it's basically saying that you're using, you know, quality components but it doesn't require tamper protection or even tamper evidence.

I have to read it a little more clearly because I was trying to listen to the call and do that at the same time and I don't multi-task as well as I used to, but I think it's going to turn out to be not all that critical.

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

Okay.

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

They way they've worded it.

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

Thank you, thank you.

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

I'll send it to the committee.

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

Thank you. Okay, it maybe...well, we'll update these and...we'll update the recommendations and we'll probably have a shorter meeting next time. We'll work with the ONC and MITRE teams to figure out what we want to include in our next agenda whether we really just want to tie up these recommendations or perhaps move onto the next topic. Does anyone want to add anything else? Lisa or any of the members?

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

No, I think this is exciting, this is absolutely needed in the community and this is going to be great.

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

Great, this has been a really useful conversation and again we really appreciate you guys dialing in and your excellent participation today.

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

Yeah, I was going to say the same thing Dixie, this has been a great discussion, so thanks everyone.

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

Yeah. Okay, Michelle do you want to open it up for public comment?

Public Comment

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

Yes, 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 at this time.

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

All right.

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

So, thank you everyone and the next meeting is December 3rd.

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

Okay, thank you, thank you all very much.

M

Happy Thanksgiving.

M

Thank you.

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

Happy Thanksgiving everyone.

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

Thank you, Happy Thanksgiving.

M

Happy Thanksgiving.

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

Yes, Happy Thanksgiving, bye-bye.

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

I'm a gastroenterologist, just don't eat too much.

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

Yeah.