

**HIT Standards Committee
Privacy and Security Workgroup
National Strategy for Trusted Identities in Cyberspace (NSTIC)
Virtual Hearing
Transcript
March 12, 2014**

Attendance

Members present:

- Dixie Baker
- Mike Davis
- Lisa Gallagher
- Peter Kaufman
- Leslie Kelly Hall
- David McCallie
- Walter Suarez

Members absent:

- John Blair
- Tonya Dorsey
- Chad Hirsch
- Ed Larsen
- John Moehrke
- Sharon Terry

Presentation

Operator

All lines are bridged.

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

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

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

I'm here.

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

Hi Dixie. Walter Suarez?

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

Yes, I'm here.

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

Hi Walter. Chad Hirsch? David McCallie?

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

Good morning.

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

Good morning David. Ed Larsen? John Blair? John Moehrke? Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Here.

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

Hi Leslie. Lisa Gallagher? Mike Davis?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

I'm here.

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

Hi Mike. Peter Kaufman?

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

I'm here, good morning.

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

Hi Peter; good morning. Sharon Terry? Tonya Dorsey? And we had also invited some of the other workgroups. Are there other members from other workgroups on?

Anne Castro – Vice President, Chief Design Architect – BlueCross BlueShield of South Carolina

Anne Castro.

Lorraine Doo, MSWA, MPH – Senior Policy Advisor – Centers for Medicare & Medicaid Services

Lorraine Doo.

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

I heard Anne Castro was there somebody else?

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

Wes Rishel.

Lorraine Doo, MSWA, MPH – Senior Policy Advisor – Centers for Medicare & Medicaid Services

Lorraine Doo.

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

And there is a female voice that I didn't quite catch?

Lorraine Doo, MSWA, MPH – Senior Policy Advisor – Centers for Medicare & Medicaid Services

Lorraine Doo.

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

Hi Lorraine.

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

Wes Rishel.

Lorraine Doo, MSWA, MPH – Senior Policy Advisor – Centers for Medicare & Medicaid Services
Hi.

Michelle Consolazio – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi Wes. Any other members?

Anne LeMaistre, MD – Senior Director, Clinical Information Systems & Chief Medical Information Officer – Ascension Health
Anne LeMaistre.

Michelle Consolazio – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi Anne. Are there ONC staff members on the line? Do we have Julie Chua?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
I have a feeling she has her phone mute.

Michelle Consolazio – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
I hope so.

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

Michelle Consolazio – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Okay, with that I will turn it back to you Dixie and Walter.

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

Okay, well thank you very much Michelle and thanks to everyone who dialed in today both those who are on our Privacy and Security Workgroup or one of the FACAs as well as the public who've dialed in, and of course our participants.

For some time now the Privacy and Security Workgroup has been thinking about the role that the NSTIC might play around identity and access management and have been asking ourselves when that role might really come into play in our deliberations around privacy and security standards and certification criteria for electronic health record technology.

These discussions have raised a number of questions about the goals of NSTIC, where the initiative is within its pursuit of those goals and when we might have sufficiently mature and implementable NSTIC-based standards and technology that we can consider for national standards.

So the objective of today's hearing is to provide the Privacy and Security Workgroup an understanding of the current status of NSTIC, the maturity of the NSTIC-based standards and technology and insights into the readiness of these NSTIC-based standards and technology to be considered in our deliberations around potential standards for identity and access management.

The hearing today will start with an overview of the NSTIC Program from the perspective of its leadership and we really thank the leadership for taking the time out to join us today to give us this context.

This overview will be followed by three panels. The first will focus on the NSTIC ecosystem, the second on the experience of pilot implementers and the third on some perspectives from the healthcare industry.

Each panel will begin with individual testimonies that respond to a set of questions that we provided ahead of time and following the prepared testimonies the members of the Privacy and Security Workgroup and FACA members who have called into this hearing will have an opportunity to pose their own questions.

Walter and I will serve as the moderators and Michelle Consolazio will be our timekeeper. So we request that each speaker respect the time slot allotted to their testimony and we also ask that our Workgroup members use the raise hand functionality that's available in your browser to let Michelle know that you wish to speak it's in the top gray bar on the left you will see a little icon of a person with their hand up. So, please use that and Michelle will recognize you and call on you to ask your question or make your comment.

We offered our panelists the opportunity to provide written testimonies and all the written testimonies that we've received are in the downloadable materials, PDF file that's downloadable from your web browser. As we begin our hearing we do want to thank all the individuals who have agreed to share their experiences and thoughts and insights with us.

We know that you've put in a lot of time on this testimony and looking at our questions and we sincerely appreciate your time and sharing your knowledge with us because your knowledge and your understanding will really be helpful to us moving forward in consideration of NSTIC. So, with that Walter would you like to add anything?

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

Yes, thank you Dixie. I guess I would only add that this is really our first initial hearing on the subject and that as NSTIC continues to evolve and the healthcare industry continues to gain an understanding of its applicability and used in healthcare identity management I think we will be considering convening potentially follow-up hearings on the subject down the road.

I also want to add my thanks to all of the members of the team that helped put together this hearing. It has been quite an undertaking actually as it turns out and we tried different dates and times and so thank you so much everyone for your time and your willingness, to the testifiers, to participate and to share their knowledge and experience on this subject. So, I'll turn it back to you Dixie now.

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

Okay, yes, I want to share Walter's thanks to those who dialed in and want to tell those of you who are dialing in from the West Coast you're not the only one I too am here at 7:00 o'clock in the morning and I know Wes is, so you're not the only one. So, with that let's proceed to our first hearing or our first panel if that's okay. Michelle do you want to say anything more?

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

No. I think I'm good. I think now it's just a matter of whether Jeremy will be available.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

I'm here. I found a way.

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

Great.

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

Great.

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

Thank you very much, thank you. As I mentioned earlier the first panel today will give us an overview of the National Strategy on Trusted Identities in Cyberspace and give us their perception of the current status of the development and implementation of the vision and the various standards that they've developed.

Our first speaker is Jeremy Grant who is the Senior Executive Advisor on Identity Management for the National Institute of Standards and Technology. And since the beginning, I believe, Jeremy has led the NSTIC Program for the White House and for NIST and we feel very, very privileged to have Jeremy join us today.

Following him will be Peter Brown or will be Tom Sullivan, the Chair of the Healthcare Committee of the Identity Ecosystem Steering Group which is IDESG, Identity Ecosystem Steering Group, and he will give us the perspective from the healthcare committee of that group.

And then finally we'll hear from Anil John who is a Security Expert at the General Services Administration and he will talk about the FICAM Trust Framework Solutions Program at GSA and how it plays a part in the NSTIC Program. With that I'll turn this over to Jeremy.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Well, thank you and good morning and thanks to the Members of the Committee and the Workgroup for inviting me here today to talk about the National Strategy for Trusted Identities in Cyberspace or NSTIC as it's known.

I lead the National Program Office that was established at NIST to lead implementation of the strategy. I'm very excited to see this committee choosing to focus the better part of today of the topic of trusted identities in cyberspace.

Next month will mark three years since President Obama signed the NSTIC and as has been discussed in previous hearings NSTIC is a national initiative that calls for the government to collaborate with the private sector to raise the level of trust in online transactions in a way that improves privacy, security and usability for all Americans.

While a government issued strategy NSTIC calls on the private sector to lead its implementation driving creation of a vibrant identity ecosystem where individuals and organizations will be able to trust each other because they follow agreed upon standards both technical and policy to obtain and authenticate their digital identities.

In very simple terms, NSTIC seeks to catalyze a vibrant marketplace where all of us within a few years can choose from a variety of different types of advanced identity solutions that we can use every place we go online in way that's more secure, more convenient and more privacy enhancing than the password centric systems we use today.

For healthcare where the promise of electronic health records largely depends on trust for EHRs to reach their full potential we think NSTIC is especially important.

At a time when passwords are the number one vector of attack and data breaches, note that 76% of all breaches in 2012 were executed by adversaries exploiting the various weaknesses of passwords, and identity theft in all sectors including health is a major issue NSTIC lays out a path for the creation of market-driven standards-based solutions that will enable health providers or patients to easily log into electronic health records in a way that ensures good security and protection of privacy.

Among sectors participating in the implementation of NSTIC health has been at the table, although, as I will detail today there is a lot more that the health community could be doing to help advance the implementation of the strategy and there are very material reasons why health should be doing more.

At the end of the day my view is the success of electronic health records will be largely dependent on whether providers and patients are willing to trust them and whether they're easy to use. Particularly for patients the idea of enabling initiatives like Blue Button that allow patients to easily download their health data and share it with others is exciting but the full potential of these initiatives will only be realized if patients have an easy way to assert that they really are themselves online and not the proverbial dog on the Internet.

Protecting sensitive personal information with passwords is akin to building a massive stone fortress and then securing the front door with a kind of lock I use to keep my 2-year-old out of my bathroom.

NSTIC lays out a path to solve this challenge enabling providers and patients to easily and securely logon to multiple health applications in the cloud without having to go through the hassles and costs of obtaining a new credential.

Now identity is certainly not the only layer of security needed but it is one of the most important. And given the need for the end user to play an active role in asserting his or her identity it can be one of the trickier layers to implement.

The solution can't simply be secure it has to be easy to use or else users just won't bother. Solving what we often refer to as the identity conundrum is not something that can be easily done by any one player or sector it requires collaboration across many types of stakeholders to craft scalable, standards-based solutions that are interoperable across sectors.

NSTIC calls for a voluntary multi-stakeholder collaborative effort to tackle this challenge and if there's one message I'd love to leave this Workgroup with today is that voluntary efforts do not succeed without committed volunteers. I hope that today's hearing will lead to actions that help to increase the commitment and involvement of stakeholders in advancing the NSTIC.

Now as we approach the three-year anniversary of the strategy there is a lot of good progress to report. First there are 12 NSTIC pilots helping to see the marketplace of trusted identity solutions and tackling barriers that the market has to date struggled to overcome.

Six of our 12 pilots have some nexus with health applications you'll have the chance to hear from some of them today. Our office just last week closed out our most recent pilot's solicitation round, 42 applications were received, we expect to make another round of awards in September.

Second, the Identity Ecosystem Steering Group or IDESG is working to craft a framework of standards, policies and operating rules to support the ecosystem. Key to implementation of the strategy was the creation of a privately led steering group that would bring together stakeholders from across the spectrum to oversee the process for policy and technical standards development.

The steering group first convened in August 2012, today it has more than 200 members who are collaborating each week to advance the implementation of the NSTIC. Membership is really quite diverse. The board alone includes representatives from firms like Oracle, Aetna, LexisNexis, Neiman Marcus, Gemalto and Salesforce as well as advocacy organizations like the AARP and the Electronic Frontier Foundation.

The diversity of participants is quite remarkable as is the fact that all of the parties I just listed not only agree on something but are all working together to advance it that's something that's rather rare in these times.

Since its establishment the IDESG has established a priority action dashboard of deliverables needed to create the identity ecosystem framework and is making good progress against it. Among early activities the steering group has developed a functional model to find core use cases and developed a novel privacy evaluation methodology or PEM that's being used by many NSTIC pilots as a way to evaluate the different privacy risks of identity solutions.

Of note the IDESG is also incorporated as a 501(c)(3) not-for-profit and is preparing to start raising its own funds.

Among the early sector specific groups to form an IDESG was the Healthcare Committee you'll hear more directly from its Chair, Dr. Tom Sullivan later today. It's fantastic that the Healthcare committee exists although I'll note, if you look at the participants, and I included a link to it in my written testimony, many major players in the health sector are not at the table. Given how important an issue this is for the success of Health IT we'd love to see broader involvement here.

I will note an encouraging note at HIMSS last month announced the formation of a new Secure Identity Taskforce that will work very closely with the Identity Ecosystem Steering Group and I'm hopeful that this may help to attract some new players.

Third, the federal government is helping to drive the identity ecosystem by making some major advances in its use of online identity and federated identity in particular.

As background NSTIC specifically called on the federal government to lead by example on NSTIC being an early adopter of the ecosystem and the services it provides the citizens and businesses online. Key to this is finding an easy way for agencies to actually integrate with a growing array of externally issuing credentials that have been approved for US government use under GSA's FICAM Trust Framework Solutions Program which my colleague, Anil John, will discuss a little later today.

This approval program is one of the first of its kind and it's a very important step in the government demonstrating the feasibility of actually accepting identity solutions that are not its own. The government is somewhat blessed to have 12 approved identity solutions today with several more in the pipeline. These solutions range from PKI solutions on one end down to OpenID-based solutions at the lower levels of assurance. Agencies have made clear that integrating with 12 solutions is no picnic. They have been asking for a solution to simplify it.

So, the upcoming launch of the Federal Cloud Credential Exchange or FCCX as its known is specifically designed to address the simplification issue and its launch will be a key milestone for the NSTIC. Doug Glair from the US Postal Service will tell you more about FCCX later today but I would suggest the key take away for this committee is that FCCX represents the kinds of commercially available identity hubs that are out in the market today as a solution for helping online service providers integrate with a variety of different identity solutions. As the health sector looks for ways to help providers both big and small and patients join the identity ecosystem we believe identity hubs are likely to play a major role.

Fourth, we're seeing the marketplace respond to NSTIC's calls for better standards and interoperability. February was a particularly great month with two major new technical standards advancing in the world of online identity. The first was the formal finalization as a standard of the OpenID Connect which provides a strong authentication layer on top of the widely used OAuth 2.0 standard.

And the second was the release of the draft FIDO specification, FIDO stands for Fast Identity Online, which essentially aims to create a wrapper that will enable online service providers to leverage the dozens of different alternatives to passwords for authentication that are in the marketplace through a standardized approach.

Now as you'll hear today we still have more work to be done on standards but these are two industry-driven advancements that together go a long way to providing a better technical foundation for the identity ecosystem.

So, as we have this hearing today it's now more than 2 years since this Workgroup last held a hearing on NSTIC. As a result of that hearing a decision was made to upgrade security recommendations for health providers to include multifactor authentication. And the recommendations called for ONCs work on providers to be – I think the quote was "informed by NSTIC." Likewise the Workgroup recommended ONCs develop and disseminate best practices for patients that among other things were consistent with NSTIC.

Now a key driver in these recommendations, two years ago, was that the strategy had just been launched and the committee was a little reluctant to recommend specific actions around solutions that did not exist. This was not an illogical outcome. It would be hard for this Workgroup to recommend the adoption of technologies or processes that are not yet widely available in the marketplace.

That said, if the Workgroup or the broader health sector are of the view that this marketplace will soon be created while everybody simply sits back and watches I think you all are going to be waiting for a long time. As I noted earlier today, voluntary efforts do not succeed unless people volunteer.

NSTIC will only be a success if sectors that are in need of better identity solutions step forward and demonstrate a willingness to roll up their sleeves in support of a collaborative effort. Likewise, if every sector takes a wait-and-see approach it's quite certain we will not get very far.

So, I would suggest that this Workgroup and indeed the health community as a whole look at NSTIC not as a program but rather as an opportunity by throwing down a marker for the future identity ecosystem that was embraced by industry and advocates alike President Obama created an opportunity to change the marketplace.

And by funding NSTIC congress created an opportunity for pilots to test new better approaches to online identity as well as a venue in the Identity Ecosystem Steering Group for stakeholders across different sectors to work together to advance the marketplace. Now these are not the kind of opportunities that come every day nor are they ones that are likely to exist in perpetuity.

To capitalize on the opportunities stakeholders must decide to seize it which may mean that they actually step up to the table and proactively engage to make the vision laid out in NSTIC a reality. Given what's at stake I hope to see much stronger involvement from the health community over the next year.

NSTIC offers an opportunity to help inspire patients and providers to trust in electronic health records and to empower them to leverage EHRs to play a bigger role in their care. If they come, we can and will build it. Thank you and I look forward to your questions.

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

Thank you very much Jeremy that's a very useful update and you certainly did an excellent job in laying the groundwork for the next two talks that come after you one from the IDESG Healthcare Committee and the other from the FICAM Program at GSA. So, thank you very much. And I remember well your testimony, your initial testimony at our public hearing about, what is it about a year or so ago two years ago?

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

I think about two years ago.

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

Yes, yes and so thank you very much for joining us today again.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Thank you.

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

Okay, our next speaker is Tom Sullivan. Tom?

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

Yes, can you hear me all right Dixie?

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

Yes, thank you.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

Okay, you're welcome. Well, I did present my remarks in written form so I hope people, if they don't understand what I'm saying or have trouble hearing, will be able to download them. But, let me depart from the written remarks just for a minute because, you know, what I have to say is as much related to policy as it is to standards.

But I first want to say it's pretty rare that a physician would agree with anybody else about anything but I have to say that I am 100% behind Jeremy's remarks and he's been an exemplary leader of our movement over the last 18 months where I've been active.

So, the most important thing I would say, my advice to take away from this, I completely agree that we need to collaborate more between commerce and HHS or the Office of the National Coordinator. We've been – since we've had our committee we've slowed down a little bit in part because we need much more participation especially from the major players in healthcare.

And look I've been a physician for 40 years, I practiced in a very large health system in Boston and I've been involved at the national level with this.

So, this effort is going to take a long time where we're talking about trusted identities in cyberspace and moving it into the healthcare area. So, we need much more interaction between ONC, your committee and also frankly the CMS and Medicare provider enrollment area, we just need to encourage much more participation.

So, I'll start a little bit now with the remarks that I wrote and I just want to give you this caveat that this is my personal opinion as chair of the committee for the last 18 months, you know, I think I understand the sense of the committee but don't mistake this as something that – not everyone on the committee would always agree with every single thing that I say.

But, again, I think it's fair to say that everybody on the committee endorses the NSTIC principles, the privacy enhancing, the interoperability, the secure and resilient credentials, the easy-to-use things that Jeremy outlined in his introduction.

So, focusing just on the trusted identities we believe there are far too many examples of unnecessary redundancy and identity proofing and management of both providers and patients and this leads to higher cost, inefficiency, errors, fraud, frustration throughout the industry despite an almost universal agreement and the need for simplification.

Privacy and interoperability are among our most pressing concerns and they often conflict where implementation in the real world of competition, multiple vendors, multiple standards, complex user demands for control and especially in healthcare heightened liability for errors and they're all factors that we're obliged to consider.

So to briefly illustrate the problem I've simplified this into two scenarios and they might be oversimplified.

In scenario one the patient is in total control of his or her identity and decides what, when and with whom any and all information is shared. Now this scenario represents enhanced privacy for the consumer but it adds the risk of danger and harm if the information associated with a particular identity is incomplete, misleading or not shared appropriately. For the best results this scenario implies very active patient engagement.

In scenario two, the enterprise or the provider practice, the physicians, the health care system they control the identity attributes of the patient with the associated advantage of convenience and efficiency for the treatment and the administrative professionals or I'd say TPO and HIPAA language. There is also a certain element of patient safety added in this scenario since it is easier to discover aggregate data that might bear on treatment decisions.

For example, a more comprehensive and accurate medication list, procedure history, lab results, etcetera. However, in scenario two the patient does lose a certain element of control regarding data sharing and thus perhaps less privacy protection.

Now outside these two scenarios it's likely that given the rapidly growing trend of consolidation in medical practices within large systems and in large groups corporate attorneys are very likely to play a much larger role in the future of influencing how healthcare identities are managed.

In Massachusetts, my own state, it's currently estimated that up to 75% of all providers are employed by these large entities or enterprises. That's a huge change over the last 20 or 30 years.

We on the committee discuss these issues at length and we presented a very small number of use cases with many more in the wings both from within our committee and from others in the IDESG outside the healthcare environment and yet they are equally concerned with privacy, interoperability and the implementation of the other NSTIC principles.

In simple language we tried to model a use case of identities in the environment of a record locator service or relationship locator service that it could include delegation of authority. It's still in a draft form though we've had it published on our IDESG wiki since mid-December and we present an excerpt which I included at the bottom of my written material.

We welcome all comments and suggestions for improvement and once again I'll say we request more interaction and collaboration with both ONC and particularly with the provider enrollment area in Medicare.

I can go on and discuss a little bit of this – again at the bottom of my remarks I have something titled a brief discussion of data segmentation and multiple and unverified IDs. I’m not sure if I’m over my time limit but I will say just to summarize it very quickly in the very last paragraph of the section I referred to that if we have multiple identities because we do talk a lot in IDESG about pseudonyms and anonymity but I think that presents some particular difficulties in terms of the risk of danger in healthcare and patient harm.

So, if we do allow for unverified IDs when a patient is presenting to a health care system I think it's important that both the patient and the physician have a discussion about the risks and the dangers of unverified IDs where someone is basically hiding essential information from a treating physician.

So, I sum this all up, and again, I’m abbreviating the remarks, by saying that a healthcare provider who is unwilling or unable to accept the potential liability of treating a patient who presents with multiple or unverified IDs for healthcare purposes for non-life-threatening conditions should not be obligated to provide care under those circumstances.

Again, that’s a quick summary. I encourage you to read the rest of the use case. It’s also online in our IDESG wiki and I’ll stop there and entertain any questions just as Jeremy or wait for the next presenter. Thank you.

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

Thank you Tom we really appreciate your comments and we also appreciate your written testimony. And we are holding all questions until we hear from all three panelists. Our third panelist is Anil John from the – a Security Expert in the General Services Administration. Anil?

Anil John – Digital Security Expert – General Services Administration’s Office of Governmentwide Policy

Thank you, good morning members of the Privacy and Security Workgroup. I serve as the Program Manager for the FICAM Trust Framework Solutions Program. FICAM is an acronym for Federal Identity Credential and Access Management.

I’ll start with the motherhood and apple pie reality that the Internet has transformed the way that we conduct day-to-day transactions it allows us to take advantage of the convenience and flexibility online services offer. These same expectations of ease and flexibility are something that citizens and businesses now have when they transact online with the federal government. However, high-value transactions delivered remotely are particularly exposed to security vulnerabilities.

So, in order to mitigate the risks involving valuable resources and very sensitive personal information, identity is at the core of most government processes. Once identity is established all subsequent government online activities ranging from providing services to granting benefits and status rely on that accurate and rightful use of that identity.

Since 2003 government-wide policy has called for reducing the burden that is placed on the public when they interact online with the government by allowing citizens to use credentials that same might already have.

The FICAM roadmap and implementation guidance, which government agencies are required to align with, calls for the establishment of a federated identity framework for the US government to implement this policy.

The Trust Framework Solutions Program is that federated identity framework for the government and is the implementation of the NSTIC within the US Federal Government. There are three aspects to the TFS Program that I wanted to draw your attention to.

First and foremost it seeks to leverage the innovation in the private sector by utilizing credentials, tokens, identity services that citizens may already have provided they meet the government’s security, privacy and interoperability requirements.

Second, it acknowledges and addresses the inherent limitations of a direct certification program by the government. It does so by seeking out sectors, organizations, communities of interest that have existing assurance frameworks, legal frameworks, certification processes, the combination of which is also known as cross frameworks and adopting them if they can meet the government's requirements for security and privacy. The end result is that a service that is certified by an adopted trust framework provider is comparable to a government certification and as such can be trusted.

Finally, experience has taught us that security and privacy policy compatibility does not equate to "on the wire interoperability." As such we have put into place mechanisms to address this particular point. These include the ability to create from scratch profiles of protocols or to adopt industry-based profiles after a security and privacy and interoperability evaluation. And even more importantly we have implemented verification testing to ensure that the services are implementing these profiles as part of the approval process.

Ultimately, as Jeremy noted in his introduction, the TFS Program is the mechanism by which the government accepts full use identity solutions that are not its own. As such, it fulfills the role – as such it fulfills government's role in the private sector led identity ecosystem by being an active member and a consumer of services as called for in the NSTIC. Thank you and I look forward to your questions.

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

Thank you. And now I think we're ready to open up the floor for questions from the Working Group. So, Michelle, would you call our first question and from other FACA members who might have called in as well?

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

It looks like Walter has a question.

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

Oh, well, okay, thank you. This is Walter, I get the first question, thank you. This has been a terrific overview thank you so much to the three of you. I have two very quick or hopefully very quick questions.

One is regarding, well the reality that of course eCommerce is global and so my question goes around how is this entire activity – or how do you see this entire area of identity management evolving in other countries? And do you see any international efforts under way that will help ensure that our NSTIC efforts are interoperable beyond our borders I guess? That's the first question.

The second question is I think we heard a few of the things that have worked well in the development effort of NSTIC. So I wanted to ask if you can mention a few other things about your perspective on what has worked well and what has not worked really as expected and what are the, you know, some of the things that are being done to help continue to advance this effort in terms of ensuring that, you know, things are working well to move it forward? So, those two questions, thank you.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Shall I start? This is Jeremy.

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

Thank you, Jeremy.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Yeah, so thanks for the questions. The international aspect is a great question and it's actually one that's quite important, you know, we point out that while the "N" in NSTIC stands for National this is something that we really can't develop in a vacuum here in US given that, you know, the Internet is global and the types of transactions that we're all engaged in are global not to mention if we're looking for the private sector to lead they are much more interested in international approaches than country-specific approaches.

The Identity Ecosystem Steering Group first of all is worth noting is, you know, basically free for anybody to participate in and is open to anybody around the world and we've been blessed to have participants from more than 12 countries playing an active role.

The group has an international coordination committee that's actually looking, among other things, at how activities that are going on within that steering group in support of the NSTIC can also be coordinated and aligned with different efforts around the globe.

It's also worth noting that, you know, NSTIC as, you know, sort of a marker has, you know, had quite an impact in other countries. Anil and our – from GSA in our office hosted just a couple of weeks ago what was a third and what's been a series of international identity summits that's been government only, we had eight different countries here ranging from the UK where their identity assurance program very closely tracks the NSTIC, they even joked at one point they took our strategy and, you know, added an extra "U" to words like flavor and color and have sort of run with it. Israel, Japan, Canada, Mexico, New Zealand, Denmark all were also participating in the event.

And I would say there is a lot of, you know, not everything is going to perfectly align globally right from the start but there is a lot of interest among different countries and looking for ways to make things align.

And certainly when it comes to, on the standards side, you know, I mentioned earlier, you know, new standards efforts like OpenID Connect and the FIDO Alliance, you know, both of those are really looking at things on a global basis, in fact you'll hear from Nat Sakimura later today who is based in Japan and, you know, from there has driven a lot of the work around OpenID Connect and other standards, and, you know, likewise that this really has been sort of a global effort.

And so I think on the technical side there is some good foundations that are in place that are really focused on interoperability.

And I can – oh, I should also note Peter Brown was on the agenda as well to talk along with Tom Sullivan about the Identity Ecosystem Steering Group, Peter's notable both for being Chairman of the Board as well as being a Brit, as Peter notes, a British Citizen with a Belgian ID card who lives in Los Angeles, as an example of the global nature of this effort.

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

Thank you. Does this international effort have a different name with the – you know, besides NSTIC? Is it called something different at the international level?

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

No, it's really more – I mean NSTIC is, you know, the National Strategy that President Obama signed I think there is an International Coordination Committee in the Identity Ecosystem Steering Group that is focused on these things and it's, you know, focused both on NSTIC as well as, you know, broader identity efforts around the world.

But, you know, in the UK they call there's the Identity Assurance Program, you know, other countries have their own names.

I think the bigger theme to take away is that a lot of countries are – especially in the wake some national ID programs perhaps not delivering the types of things around citizen identity, consumer identity that people had hoped looking at ways that federation efforts like NSTIC, you know, how do you look at, you know, our guiding principles and our vision as something that can be replicated in other places.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

Can I add a little bit to what Jeremy just said Dixie, this is Tom Sullivan again?

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

Yes, please do Tom.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

So, in our over the – again, over the last 18 months in healthcare we've had a number of discussions with different experts who have come together in the IDESG group and one of them is – we're very interested in what the postal service, the US Postal Service is doing with the Federal Cloud Exchange.

We would love to see the postal service and their ability, their long history of international contracts with other postal services in other countries that helps them enforce the law and sort of bring that trust and the prosecution of fraud into the private sector in the United States that might ultimately get into the international sector.

So, I guess what I'm saying here is if you can advocate for congress to act to help the postal service get more involved with trusted identities and use their ability both nationally and internationally to help create an additional bulwark or a barrier to fraud and abuse I think that would be great.

The postal service and their FCCX, and I think you're going to hear about that a little bit later in one of the panels, I think that's another example of a pilot even though it's run by the postal service and Jeremy mentioned several other pilots that are developing that I think will show us the ability to do this on an international level.

The final thing I'll say is in the private sector also where I work I'm very familiar with the very, very tough credentials that physicians must satisfy or meet in order to prescribe controlled substances electronically and it's just a shame that we cannot easily reuse those credentials once we have identity proofed people. But we are exploring some international areas where we might be able to carry that out also. So I'll just end it with that.

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

Yeah, thank you and yes we're going to hear about the FCCX Program, the postal service program, in our panel two later, I think it's 12:05 today. So, we will hear about that later. Are there others who have questions for our panelists?

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

Yes, there are a number of people in the queue. So, we'll start with David McCallie.

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

Good, yeah, can hear me okay?

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

We can hear you.

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

Good, David McCallie, my question is – as maybe a little abstract and I might have trouble posing it but I'll give it a shot and I'll target it to Jeremy but I think maybe Dr. Sullivan would have some thoughts as well.

And the question is regarding the distinction between NSTIC and its associated efforts providing sort of an enumeration of people versus NSTIC providing the ability to prove that someone is who you think they are.

And what I'm getting at is I'm hearing in some of the comments suggestions that NSTIC would lead to the solution of an enumeration of all patients, a national patient identifier for example or the enumeration of all citizens which obviously in some countries is coupled with the identity service, but I would just like clarification that that's not what NSTIC sees as its target and that existence of NSTIC in a well-functioning mode would still leave you with the question of who are the people that I need to identify and prove and how do I map them to my internal systems?

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Yeah, I think that's a great question and I can clarify. So, NSTIC is by no means is it a national identity program it's a digital identity strategy and, you know, at the end of the day, you know, I describe it as a way, you know, as I said earlier to catalyze the marketplace where consumers have choice to, you know, obtain a credential that they can use when they go online for experiences that are more secure, more convenient, more privacy enhancing than managing 25 or 30 different passwords.

But, I think it's, you know, worth noting that, you know, even if we're wildly successful and, you know, I never really answered Walter's second question in terms of what's going on, you know, what's going well and what's not, but I think we're in a pretty good place right now relative to, you know, the scope of the challenge and, you know, the resources, you know, we have to drive things forward.

You know you will still have, certainly in the United States, people who will probably not have a credential just like you have people in the United States who in general do not go on the Internet for much of anything these days.

So, you know, the idea is if you can at least eliminate some of the barriers, you know, to this marketplace or different credential providers and, you know, perhaps, you know, come up with some incentives in the marketplace as well for, you know, people to actually get them and use them then we at least drive some material improvements above where we are at today.

The identity proofing side of it is an important part of it particularly as you start looking at, I guess what I would consider higher risk transactions, you know, right now there's things that I do online where it's perfectly okay to be the proverbial dog on the Internet, you know, if I'm, you know, leaving, you know, a very politely written, you know, comment at the end of somebody's blog or news article it doesn't really matter if, you know, they know that I'm Jeremy Grant or I could say I'm, you know, Bozo the Puppy Dog.

And, you know, likewise if I'm actually, you know, logging into, you know, a hospital to, you know, download some health information there you actually want to make sure that there is some proof that I really am me and not somebody who is simply claiming to be me.

And so I think a part of the challenge with this effort to create an identity ecosystem is how do you give people not only strong credentials, you know, things that go beyond passwords but also bind them to proof of identity so that when they are engaging in transactions where there's a higher risk profile you are able to get those attributes about them that you actually need to be assured that they really are who they claim to be.

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

So let me run on that and push the question to Dr. Sullivan and the Workgroup, the Health Workgroup. Is the approach to focus on interoperability of these systems so that someone who has been proofed by one system can validate themselves through another system or is it in fact to enumerate the people that need to be proofed?

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

This is Michelle, Tom before you answer, I think Peter Brown is on as well, is he here to help answer questions with you and if so I just want to make sure that he knows that he has the ability to do that?

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

That's correct, yes I'm here, I'm listening, thank you.

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

And, yes, this is Walter, I wanted to jump in I'm sorry to interject, to Peter, we really apologize I'm not sure what happened with the agenda there but we will ask you to make your remarks at the beginning of panel one if you don't mind.

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

That's fine.

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

But you can certainly participate in this discussion, absolutely, thank you.

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

Okay.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

So if I can take a little stab at answering that question. We do strongly believe in the need for simple interoperability but it's got to be – it's got to have those – to do that we have to have these trust marks and trust anchors and the trust framework and I think that's in the process of being developed. Now it isn't the major topic of our healthcare committee discussion but it is part of IDESG.

You know we recently became a 501(3)(c) and we're looking at ways of sustainability, how this is going to continue and perhaps, and Jeremy and Peter can address this better than me, maybe we can develop a trust service or something that would help with interoperability. I don't think we're looking to – I'm sure we're not looking to provide a national ID for all patients.

First of all, you know, back when the HIPAA Privacy Rule was written that debate took place and it was decided that until congress acts we would not have a national patient identifier but we are looking at ways of being able to identify proof patients and providers, and to again make those credentials and attributes a lot more reusable. And we do make a distinction again between identity, credentials and attributes. So that's part of the discussion.

I will say I'm encouraged by the interest in some of the states and their departments of motor vehicles who are interested in getting involved more with identities in healthcare and one of the pilots, at least one of the pilots is working in Virginia with that as an example.

So, I'm not sure if that exactly answers your question but we are definitely not in the Healthcare Committee trying to come up with a national patient identifier even though some members have proposed that as one of several solutions.

Anil John – Digital Security Expert – General Services Administration's Office of Governmentwide Policy

So, let me also jump in and add a point from at least from the online government services perspective. We fully recognize that you need a range of everything from anonymous transactions to fully verified transactions and that range is broad.

We have categorically, absolutely no desire to create a one ring to bind them all from the identity perspective and there is absolutely no appetite for a government issued single credential for citizens within the US context.

One of the things that often happens in this conversation is that I think we – and Dr. Sullivan touched on this, is I think it is important to have a clear distinction between, and a separation between, you know, tokens, identity and bringing those two pieces together in order to create a credential.

And I think there is value in reusing the identity proofing capability but that should be able to be reused in the creation of multiple types of credentials. So from the perspective – and it should be under the clear choice of the consumer when they do that.

So, again from our perspective as well we fully recognize the range of transactions from anonymous to fully verified and that there is a clear separation between tokens and identity being brought together in order to create a credential.

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

Yeah, this is David McCallie again, thanks for those clarifications. I think that makes sense to me. The concern when you start drifting into things like prevention of fraud, you know, you start getting into the space of, well, how do I know this is fraudulent and it's because it's not somebody that's on my list of known people and it gets more complicated.

When it's voluntary ability to prove that you are someone who is already known to you, in other words that you're coming back to the portal and that it's your account and you own this account then it makes total sense for this interoperability to be there but it blurs into more complicated spaces where I can see we would have a harder time reaching agreement when you start talking about fraud prevention. But I'll stop and let some other people ask questions at this point.

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

Okay, thank you David and an interesting course of discussion there. Michelle, do we have other questions?

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

We do, we have Leslie Kelly Hall and then Peter Kaufman.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Hi, thank you all for some great information this morning. I have one clarifying question and then another. Someone just mentioned that they had formed a 501(c)(3) to establish a trust framework. I wondered who the "we" was in that? That was my first question.

And then the other, I was so encouraged to hear about this work being done with patients in mind and wondered if the approaches that you were taking were based upon some sort of professional status or if this is more of a person centric approach that says people have access to have the ability to do certain tasks in healthcare some of which require a high degree of identity proofing and credentialing, some of which don't, if you could speak to that a little bit in general I'd appreciate it. Thank you.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Sure, this is Jeremy I'll jump in and others can as well. So, I mentioned the 501(c)(3) one of, you know, the key pillars of NSTIC implementation, the strategy being a privately led effort called for the creation of a steering group that would basically focus on, you know, creating a framework of standards and policies to support the identity ecosystem that the president's strategy calls for along with an accreditation process for providers that are in it.

We initially, back in August of 2012, helped this group essentially convene, get off the ground by putting out a two-year grant to a private firm to basically serve as the convener and creator of it, but, you know, the whole idea was that, you know, they would work almost from the day they convened to transition to being more independent, more self-sustaining.

So, the group, the Identity Ecosystem Steering Group became IDESG Incorporated back in October as a 501(c)(3) not-for-profit. We're getting ready, from our office, to put out a new grant that will be likely awarded, you know, to that successor organization, you know, to help to continue to fund program activities but they're also looking to start to raise private funds.

The second question in terms of – if I think I, you know, understood it right, I think the simple answer is yes everything we're trying to do is very person centric or user centric in terms of, you know, I think the vision with NSTIC, you know, is that I would have a trusted identity provider that would have certain, you know, they would validate certain attributes about me, you know, essentially, again to prove I am really am, you know, Jeremy Grant and not only a Jeremy Grant but the Jeremy Grant who lives at a certain place in Washington, DC and is of a certain age and things like that.

And then they would assert those attributes on my behalf when I engage in on line transactions so that if I'm showing up, you know, I'll give you an example, of, you know, a challenge that the Department of Veterans Affairs has, you know, they may have 20 different Jeremy Grant's in their system if I'm going to show up with my credentials that I have at the VA and say, please let me access information involving my benefits they need to go through identity resolution, you know, which Jeremy Grant is this coming in and by asserting several key attributes they can, you know, sort out quite quickly how to match that credential to the record that they are actually carrying.

The part of what we're trying to focus on as well is data minimization, how do we limit those data request to, you know, the minimum number of attributes about somebody that are actually needed for the purpose of a transaction rather than a lot of the default of what we see today which is data broker sharing essentially everything about you often much more than is actually relevant to the transaction at hand.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you I have one more clarification. I was really trying to get to the level of assurance required and is this a one-size-fits-all for patients and providers or is this some sort of gradation that's being recommended or thought through in this group? Therefore it's a –

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

So the group –

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, go ahead.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Yeah, great question. So, I think the answer there is it's not one-size-fits-all, you know, as I said earlier sometimes it's good to be a dog on the Internet and sometimes the transaction is not online because the service provider has no way to verify that you're not a dog.

So, you know, the federal government, you know, prescribes four levels of assurance it goes back to, you know, OMB Policy dating back to a 2004 memo and, you know, NIST backed up those four levels of assurance with Special Publication 800-63 which essentially lays out, you know, guidelines for what agencies need to do at each level of assurance, but, you know, as we always point out the special publication was designed for the federal government.

And there are some things about it that may not necessarily work perfectly in the private sector and in fact, I think this Workgroup two years ago when it made recommendations on the use of multifactor authentication for health providers pointed out you want them to have credentials or tokens, I should say, that were multifactor that aligned with what was called out in Special Publication 800-63, but there was an identity proofing side of that the committee decided it didn't actually need to be in the recommendations and that there was sort of an assumption that with most healthcare providers they've already been identity proofed through some other channel.

And so – and in fact 800-63 has since been updated to also reflect that, you know, ability to sort of break apart the identity vetting versus the token strength of the solution and allow it to be more component sized.

Anil John – Digital Security Expert – General Services Administration's Office of Governmentwide Policy

So, let me add on to that as well. The only point that I would add onto that is, Jeremy is absolutely right from the perspective that there is obviously some guidance that is especially binding on government agencies, but at a high level the use of identity is entirely contextual and it has to be based on a risk-based assessment that you do in order to determine the requirement of the assurance level that you need in an identity as a first step.

Again, you also need to have a clear separation between the identity, you know, who are you versus what you're allowed to do and I think, especially this community understands that very clearly. So, there is no one-size-fits-all and it needs to be contextual and it needs to be risk-based.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

Let me just add to what was just said. Hospital identity proofing for physicians to get on the staff is a perfect example of what was just mentioned, you know, just because I'm on the staff of a hospital it doesn't mean that I can perform neurosurgery but I can do cardiac things.

And so there are a bunch of things within a hospital setting that just point this out as examples. I have not only my identity but credentials in certain areas and then privileges in other areas too. So it ties into what we're talking about making that distinction between and among identities, credentials, attributes, tokens.

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

Could I – this is Dixie, Tom could I ask a follow-on question about that just for clarification, these privileges and attributes and roles are – they are not held in the credential itself right? They're just held by the system, they're still held by the system but associated with the authenticated identity which is proven by the credential is that correct?

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

Yes, but I think that's going to change. I think, you know, the future is cyberspace management of identities and credentials and right now you are correct they are sort of held on paper or they're just – it's the old fashioned way, well, the Chief of Surgery knows that you've been privileged to do this particular procedure and not that particular procedure so that's the way that it's done now.

But in the future I do see these attributes being held more in cyberspace whether it's through tokens or whatever.

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

Dixie, this is Michelle. I just want to do a quick time check. I know Peter Kaufman has a question and we also need to get back to Peter Brown.

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

Okay.

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

So, I think that we need to transition to Peter's question quickly.

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

Yes, I agree.

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

Thanks. I was – this is Peter Kaufman. I was interested in finding out a little bit more about FIDO you might have gone into more detail on that Jeremy but things were going so quickly that I was getting a little behind. The idea that fast identity online sounded very intriguing to me and I just wondered if you could briefly go into that in a little more detail?

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Yeah, I'll talk about it and I'll bet our standards panel that comes up a little later can give their own view. FIDO was an initiative launched a little bit over a year ago that actually, you know, one way I would describe it is, you know, it's sort of – it's not trying to solve the entire identity problem it's trying to focus particularly on the topic of strong authentication and how can you come up with a way to give people, you know, consumers primarily, an easy way to either have universal second factor, you know, meaning you have a password plus a second factor or a password replacement.

And, you know, one of the challenges is there are so many different technologies that are out there, I mean, just in biometrics there is, you know, a half-dozen different modalities that are in the marketplace. There are trusted elements in different devices, there are, you know, really just a lot of different approaches and how would you actually come up with, you know, I think I described it earlier as a wrapper, that would enable an online service provider to interact with and if they choose to trust could trust any of them.

So, you know, the specifications are still in draft right now but they really focus only on authentication and in fact I think, you know, there are a lot of use cases, you know, with what FIDO looks at where you could have somebody both be anonymous or operating under a pseudonym and yet still have a strong factor of authentication that could be interoperable different places.

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

Okay. Michelle?

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

We don't have any more questions Dixie. So, I think I'll defer to you, do we want to have Peter Brown go now and give his testimony and then we'll transition to the next panel?

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

Well, I do want people to have an opportunity to ask Peter questions, so let's have Walter begin panel one and we'll have Peter give testimony as part of that so that he can be part of the Q&A.

To those of you on the line my understanding was that Peter Brown was not able to make the hearing today but he was able to dial in we're very grateful to have him here. So, we will hear his testimony as part of panel one. Okay, Walter?

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

Okay, yes, thank you very much Dixie. So, we're going to start our first panel or what we call panel one really and the purpose of this panel is to help us understand the NSTIC ecosystem and the identity management standard being looked at to support NSTIC.

So, as Dixie mentioned, somehow we skipped including Peter on the first panel but in some ways we are very fortunate that he's going to be speaking as the first person in this panel one as part of really helping us understand the entire NSTIC ecosystem.

So Peter is a Founding Member of the IDESG and currently serves as Chair of the IDESG Management Council and he is also a past Chairman on Secretary of the Board of OASIS which you all know to be as a global industry consortium on standards promoting open standards.

To emphasize even that there is more of this global dimension and I think Jeremy might have mentioned this, Peter is a tenure official of the European Parliament on unpaid leave now living in the Los Angeles area. So, he really brings that international perspective as well.

Peter will be followed by Eve Maler who is a Principal Analyst with Forrester Research specializing in emerging identity and security solutions. And then we will hear from Nat Sakimura who is the Chairman of OpenID Foundation and Senior researcher of the Nomura Research Institute.

And then we will also hear from John Bradley, Senior Technical Architect at Ping identity. And our last testifier on this panel will be George Fletcher, Chief Architect of Identity Services at AOL. So, we'll go ahead and start with Peter. So, Peter go ahead please?

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

Thank you very much and sorry for the confusion here. I won't actually address all the items that I put in my written testimony because I think it's important to keep the conversation moving forward and I indeed some of the things I would've covered have already been covered in earlier testimony and in the Q&A so I just want to focus on two or three elements.

One certainly is to underline, as Jeremy, I think has amply done already, there is a national strategy, the NSTIC, for which he holds responsibility within the National Program Office and is accountable to the White House and IDESG which is a private sector led organization which has taken up the opportunity that NSTIC offers to try to deliver some solutions to the vision and goals that NSTIC lays out as a national strategy.

The – we often refer to the multi-stakeholder nature of the organization. I don't think we can emphasize this enough. There are many multi-stakeholder organizations around and often we think of these as being, you know, various stakeholders in the finance sector or various stakeholders in the IT industry or various stakeholders in healthcare or in federal or state government.

We are more than that because it's not only multiple stakeholders from within a particular type of stakeholder group but across stakeholder groups and we have groups as diverse as consumer and privacy advocacy organizations through to major Telcos, banking and finance industry people, healthcare as we've mentioned, technology solution providers, as well as policy makers in government and elsewhere.

This I think is important because one central challenge to IDESG as an organization is to address what I've often called the tension triangle. So, a tension between three often conflicting issues. One is what is technologically feasible. What technology is today or in the foreseeable future are able to deliver. What is desirable from the point of view of public policy and what is acceptable to the public to citizens, to consumers and in the case of healthcare to patients, providers, practitioners and so forth.

And ultimately, trying to resolve the tension between those three apexes of that triangle is very difficult but I think it's a major challenge. If it were easy we wouldn't be here and if it was unimportant we wouldn't be here.

I think the fact that IDESG has gone through such a long gestation period in terms of where it's trying to get to is a reflection of the complexity and the difficulty of what needs to be done.

I think the first challenge we've had is trying to identify a common language in terms of what we expect the concept of an ecosystem or an identity ecosystem even that, different people, different people involved in the organizations have different takes on what that is supposed to be.

Some would have the view that we are trying to build something new, others that we are trying to steer an existing ecosystem in a healthier way and in a way that is more appropriate to the future challenges for online identity and trust.

And I think the nature of the organization and the nature of its government structures will necessarily be a reflection of what we expect to come out of that ecosystem and I think Jeremy has spoken very elegantly to the elements there.

I think the only other couple of points I would like to raise, because these were amongst the questions which were in the set of questions to us, about the change of the federal government role.

There is no doubt that IDESG would unlikely have gotten off the ground in the way it has done if it hadn't been for the impedance and very solid support that we've had indirectly through the White House and obviously congress but more directly through the support of the National Program Office of NSTIC at NIST.

And I think what we're witnessing now is a shift from getting things started and getting things shaped and on the rails to trying to roll back their role in terms of now being – instead of driving the organization rather giving it the practical support to keep us on the rails and to give us enough momentum to get moving forward.

As has been mentioned, the IDESG initially an unincorporated organization set up just under two years ago has now moved to a formal status as an incorporated not-for-profit organization and we've been able to do that both with help from NSTIC from the National Program Office and from the quite massive volunteer effort that we've seen from many organizations.

And I think the final comment I would make is, and it comes back to a question raised earlier about international. The "N" in NSTIC refers to the national strategy so clearly NSTIC is about what is good for the United States and what is good for US citizens and consumers.

However, IDESG was scoped from the start to take on a broader international perspective and that is indeed even reflected in NSTIC in one of its goals that we should look at international aspects. But I don't think can be underlined too much.

The problem we face is that different countries – okay, it's not just that different countries take approaches to online identity and trust in different ways but they come from very different legal, social, political and economic traditions as well and very broadly I think it would be fair to characterize the US as being a country where people are relatively comfortable with having their identity managed and identity information provided by multiple often private sector providers and tend to be more cautious about their engagements with central government when it comes to identity. And it's clear it's not on the agenda of anyone to look towards a federally mandated national identity scheme.

Whereas in many other countries and certainly in countries that I'm familiar with in the European Union which come from more of a civil law tradition the core identity file of any individual is something which is actually issued and managed by government and in Europe particularly people tend to be more comfortable with their core credential being issued by a government agency or public authority and more cautious about their relations with the private sector.

So when we look at international issues trying to resolve and trying to overcome that potential conflict because of the different expectations and possibilities in terms of delivery it's a key factor in our work and I think the international coordination committee of IDESG has been central in trying to do that.

I think I will leave it there and leave it rather to the other people foreseen on this panel to take this forward. As I said I'm happy to hang around for questions for the rest of this session and other material is covered in my written testimony. Thank you.

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

Thank you so much Peter and thank you indeed for your willingness to stay and answer some of the questions when we get to the Q&A. So, this was a great way to really get us started on this panel one and sort of provide an overview of the NSTIC ecosystem. So, we're going to hear next from Eve. So Eve, go ahead please.

Eve Maler – Principal Analyst – Forrester Research

Hi, this is Eve –

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

This is Michelle before we get started with Eve and the rest of the panelist this is just a reminder that the remaining panelists have five minutes for their testimony. I will give you a 30 second warning before your five minutes is up but at five minutes I will ask you to please stop. So, go ahead, Eve, thank you.

Eve Maler – Principal Analyst – Forrester Research

Thanks Michelle. Well, thanks for the opportunity to speak with you today. Regarding identity standards and their relevance to NSTIC Forrester Research tracks open standards related to identity and access management interoperability. We define an open standard as one that was specified in the open for which the maintainers do not charge for access or implementation license fees.

For our purposes here today a standard is central versus peripheral if it tackles key NSTIC problems spaces versus adjacent spaces such as purely enterprise facing identity management or agency to agency federated single sign on.

Standards also provide differential value depending on whether they have a robust technology performance ecosystem or they have been widely adopted in the marketplace or they uniquely solve a key problem and so on. So, based on these definitions here is our current assessment.

Three standards that immediately provide high value that is central to NSTIC's mission are OAuth, OpenID Connect and JSON web tokens also known as JWT. These provide a backbone of security and portable identity capabilities.

A standard that will in the medium-term provide high-value that is central to NSTIC's mission is user managed access or UMA. Note that the UMA effort is one that I lead. UMA uniquely provides capabilities for letting an individual proactively control data sharing access and it can use an attribute-based access control model to do so.

The reason for these assessments of high-value is that these standards are both robust in terms of security and privacy capabilities and agile in terms of Internet scale, mobility and consumer and citizen applicability.

Note that UMA is less mature than the others not having reached key stability or adoption milestones yet. A standard that provides moderate value that is central to NSTIC's mission is SAML, its value is moderate because it's more friendly to large IT shops and web browsers than to smaller organizations and mobile environments so its reach has limits.

A standard that provides moderate value that is peripheral to NSTIC's mission is X.509 which of course underlies PKI technology. While X.509 is extremely valuable as a security mechanism, as an identity platform, that is to say for persistent globally reusable user certificates, it has struggled with Internet scale environments and with privacy.

A standard that provides low value that is peripheral to NSTIC's mission is XACML. While we are tracking the FIDO authentication specifications just spoken about before closely they don't yet meet our definition of an open standard.

Now regarding standards that are relevant to the healthcare industry and gaps in the standards, all of the standards that provide high NSTIC value are relevant to the healthcare industry. Modern healthcare use cases require robust security and privacy as well as Internet scaling, dynamic distributed data sourcing and participation by business players that have a variety of IT savviness quotients. These needs suggest that the emerging technologies can provide particular value as we can see in the Blue Button+ Initiative.

Two underserved areas of standardization include personal data discovery services and auditability of data access. Discovery services are required for doing a good job of finding the locations of distributed patient records.

And auditability is especially required where patients want to control or track access by third-parties whether they're family members or simply medical systems to which the patients themselves have no access.

UMA may be of particular interest because it uniquely provides a model for handling and respecting patient consent directives in a highly distributed environment. From the UMA groups analysis it also appears to provide useful underpinnings for the IDESG record locator service use case and potentially for auditability as well.

Regarding how to accelerate NSTIC both generally and in the healthcare realm we observed that adoption of the NSTIC vision has been hampered by liability concerns among potential business participants. While social login, as Jeremy pointed out, grows in popularity we see high assurance identity networks languish.

Because healthcare systems must achieve superior security, patient choice and loosely coupled systems they require answers to this difficult question. We believe the US credit card industries move to a so-called liability shift model may be useful to examine in identity trust framework efforts. And with that I'm looking forward to fielding your questions.

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

Thank you so much Eve, thanks for the testimony. So, I think we're going to go ahead and move to Nat Sakimura. Nat are you on the line?

Nat Sakimura, MSA – Chairman - OpenID Foundation (OIDF)

Yes I'm here.

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

Oh, great, thank you so much for joining us. I understand you are in Japan is that correct?

Nat Sakimura, MSA – Chairman - OpenID Foundation (OIDF)

That's right I'm in Tokyo and it's half past midnight.

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

Oh, goodness, thank you so much for joining us and so please go ahead.

Nat Sakimura, MSA – Chairman - OpenID Foundation (OIDF)

Actually I have provided some slides so it would be great if you can – yes it's there, all right.

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

Yes they are they are being displayed now.

Nat Sakimura, MSA – Chairman - OpenID Foundation (OIDF)

Right.

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

If you could let the facilitator know when to move to the next slide that would be good, thanks.

Nat Sakimura, MSA – Chairman - OpenID Foundation (OIDF)

Yes, okay. Good morning and thank you to the members of the committee for inviting me here today. I'm honored to talk about OpenID Connect in relationship with NSTIC and HIT. I'm the Chairman of OpenID Foundation but today I'm speaking on my personal capacity.

After 4.5 years of rigorous specification building OpenID Connect was finally approved as a ratified standard this February. Next please.

Yes, OpenID Connect forms and identity layer within the cyberspace. Let me explain briefly, when we speak of layers we often use something called TCP/IP reference model. This is a model that defines the communication functionality that an Internet host should have into four layers. The fourth layer is called an application layer here but this application means communication service such as HTTP and SMTP. That does not mean the applications software we use. Next please. Yeah, next please.

The application software is built on top of them. And in this figure I have depicted the IAM in italics. The reason I specifically brought it up among other functionalities is that it exists in every application software in one form or another. Next please.

Over 95% of Internet security issues stems from lousy identity and access management, what I call as IAM, right, and what we have released at this time are international standards that pulls out the functionality into another layer, identity layer, and enables software applications to form, to outsource those indications and authorizations to an external module with a standard interoperable interface.

And I have depicted in this figure here application software talks the identity layer through a well-defined standard protocol to achieve authentication and authorization safely. By extracting the authentication and authorization functionality and thus outsourcing it to a special purpose software or a service that application software can specialize on what they're supposed to do with the application functionality itself and its core components without implementing the authentication and authorization which is extremely hard to implement correctly without building the security holes into itself. Next please.

What we have raised at this time, as final, are these four specifications. OpenID Connect Core which defines a core functionality for – as an authentication built on top of OAuth 2.0 and the use of claims to communication information about the end user.

OpenID Connect Discovery which defines how clients dynamically discover information about OpenID providers for the user.

OpenID Connect Dynamic Registration which defines how clients dynamically register itself with OpenID providers.

And OAuth 2.0 Multiple Response Types which defines several specific new OAuth 2.0 response types. Next please.

So, it's an identity layer on top of OAuth 2.0. It is simple REST-based yet secure, authentication method agnostic in support of indication context and step up authentication, consent framework is built inside, it can do explicit, implicit authentication as well as revocation of consents.

And it is fair information practice principle friendly and supports access delegation or access granting so that data can be accessed without a user in presence. And it is distributed claims model can deal with multiple data sources. Next please.

Implementing an OpenID Connect is simple and easy yet secure and there are multiple open source implementations as well as commercial implementations and options for digital signature and end-to-end encryption adds to the higher degree of security. Next please.

When we were designing this new protocol we had been looking at many use cases and NwHIN related use case was one of them and here I have depicted classic Alice goes to college use case. I'm not going to explain it here but you can probably look at it yourself. Next please.

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

Thirty seconds.

Nat Sakimura, MSA – Chairman - OpenID Foundation (OIDF)

All right, next please. And it's been using Blue Button RHEX and so on and it's, you know, a pretty good starting point for these kind of things I think. So, that's all from me and the next slide only has some useful links. Thanks very much.

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

Thank you so much Nat that was really very helpful and I'm sure there will be a number of questions in our Q&A portion, so, thank you and thank you for staying this late and joining us. We're going to go next to John. John are you there?

John Bradley – Senior Technical Architect – Ping Identity

Yes, can hear me?

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

Yes we can thank you, go ahead please.

John Bradley – Senior Technical Architect – Ping Identity

All right I'd like to thank the committee for inviting me to testify today. I put in some written testimony but I'm going to almost completely diverge from that and try and cover some of the things that you guys seem to be interested in.

So, the various software providers have been participating in the various NSTIC pilots and the IDESG which are similar but not precisely the same as many of you realize. But the software industry also is involved in projects around the world, I'm personally involved in ones in the UK, Canada and many other places.

So, we rely on standards like OpenID Connect from the OpenID Foundation, SAML from the OASIS Security Services TC, OAuth from the IETF, JOSE from the IETF, etcetera for what we implement. There are questions about NSTIC standards. I don't know that there is actually such a thing. I would prefer to think of it as the IDESG, which you've heard being created as a result of NSTIC, will adopt and/or promote standards that are seen to be beneficial for the promotion of NSTIC.

So, we're not waiting for NSTIC to produce some sort of standard. Now the world gets on with these lots of deployments from the – as an example Ping ruled out OpenID Connect support over a year ago based on the implementer's drafts.

Almost all of the large commercial COTS or commercial off the shelf software providers, as the GSA likes to refer to them, you know, support OpenID Connect with few exceptions or are about to roll out, certainly the support for OAuth is very widespread now for OAuth 2. I can't think of anyone who isn't supporting OAuth 2 in their commercially shipping products and in some cases, you know, multiple shipping products.

So, because OpenID Connect is built on top of OAuth we're seeing very rapid deployment. A lot of the identity provider services that we're seeing on the Internet people like Google have already rolled it out.

I was at the meeting with Deutsche Telekom the week before last and their comment was that they had tried to connect all of their business partners with SAML and had given up and essentially moved to OpenID Connect because while they had very sophisticated IT departments the people that they were trying to connect to didn't so they had to move to a standard that was capable of more rapid deployment.

We do – you know, Eve and myself and other people, you know, have been involved in SAML for a long time it's a great standard, it's still, you know, it never really conformed to the flexibilities of the social web the social Internet required, you know, it can be modified but most people have – because most of the relying parties want both authorization and authentication the world has sort of moved on in these larger systems where you have thousands of parties that need to interconnect to where most of those people are looking at OpenID Connect and OAuth.

We also, as an example, I was at the GSMA last week which is the global telephone alliance for mobile operators and we are in the process of forming an OpenID Foundation Workgroup to set a global standard for mobile operators to provide a standardized multifactor authentication to relying parties via OpenID Connect. I think that's one of the important things.

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

Thirty seconds.

John Bradley – Senior Technical Architect – Ping Identity

One of the important things is that OpenID Connect abstracts the first mile of authentication where you're going to see protocols like FIDO, which is one of many first mile authentication protocols like mutual TLS X.509 that Eve mentioned. So, Connect is not mutually exclusive with things like FIDO they're complimentary as one of the important things to remember. Thank you.

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

Thank you, John, thank you so much for that. We will go next to George and then we'll open it up for questions. So, George are you on the line?

George Fletcher – Chief Architect, Identity Services – AOL, Inc.

Yes, I am present can you hear me?

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

Yes we can hear you well, thank you.

George Fletcher – Chief Architect, Identity Services – AOL, Inc.

All right, well, thank you very much for inviting me to testify here at this committee. I want to focus my remarks around basically recommendations within this ecosystem and identity ecosystems in general. AOL is both an identity provider and/or aligned party and in that sense, right, we've implemented both sides not as a COTS package but, you know, sort of implementations internal to our organization.

So, my first recommendation is effectively "don't be a silo." The point here is that being an identity provider is really hard and as the hackers get smarter it gets harder to be a good identity provider. And as Jeremy mentioned there have been many, many password breaches over the last year. The majority of those breaches come from somebody who is trying to be an identity provider and not really very well securing their environment.

And so as consumers we tend to use the same passwords at multiple places and the exposure of one password credential leads to compromise at multiple others and we see that here as well. So, there are many standards as has already been mentioned OpenID Connect, SAML that allow for higher level of assurance use cases.

So, I think the key here moving forward in this ecosystem is to focus on being a relying party. And there are some issues with being a relying party especially in the higher level of assurance cases. So, I think there are some gaps here but they're gaps that we need to solve rather than ignore. Such things like how does the user call your customer care service and find their record, right? What is the mechanism to identify themselves into this is them so that you can find who they are?

And you run into interesting issues in that regard and the difference between sort of privacy and pseudonymity and the basically identification right. If you have to collect attributes such as a phone number to find the user's record, right, is the phone number in some way a globally correlatable identifier. So, I think there are some gaps here but that still is the direction we need to go.

As it relates to sort of user's access to their data the focus can be on authorization and not so much on the identity part. So if we can split the identity or the authentication section from the authorization, right, it makes it much easier to outsource your identity piece and still manage the authorization. I think this will come into play significantly in the area of devices, wearables and other things that may be recording data into an EHR or other system.

Maybe the final thing, and I'll wrap up, is don't forget the user. Jeremy mentioned that user experience is very important to user adoption. I think that goes to both ease-of-use and across the systems as well as making sure that for a user it's not a disjointed experience, right, if I've got records in 15 different systems, right, how do I as a user see that in one unified way and how can I sort of manage that.

I think that there are opportunities, as Eve mentioned UMA, as an emerging standard. There are some opportunities there to maybe help with both consent policies and aggregation as well as the sort of tracking that Eve mentioned on a personal level to enable sort of visualizing who has been accessing the data while not necessarily requiring it to all live in one single location. Thank you very much.

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

Thank you so much George. This, I think, panel was really helpful in understanding first of all some of the ecosystem components of NSTIC, but more importantly trailed down a little bit into the current standards and some of the gaps and that was really our intent. So, let's open it up now for Q&A and I'll turn this to Michelle to let us know who is on the queue.

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

Thanks, Walter. Just a reminder as our Workgroup members ask questions if the people responding could just state your name first so that we are able to identify who is speaking for the transcription. Thank you very much and so our first question is from David McCallie.

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

Yes, thanks to the group for a helpful insight into these standards. Maybe my question will be directed mostly to Eve but anyone could feel free to chime in.

And it's my understanding is that OAuth requires a fair amount of, OAuth 2 requires a fair amount of, profiling and that there is a fair amount of optionality in the spec designed to allow different implementations and if you would comment on that particularly with respect to healthcare use cases.

Are you comfortable that there are well-established profiles for healthcare or is that work that needs to be done or is this a mistaken impression on my part?

Eve Maler – Principal Analyst – Forrester Research

This is Eve I will comment first I suspect others may jump in and have good data on some of the specifics, but indeed most of these standards tend to be – they're not really protocols themselves. They have a lot of optionality and different modules and so they're really protocol generators.

And I think you're right that they need to be profiled to be truly interoperable and there's a number of layers at which profiling can be valuable. Generally just to say turn up the security in a general deployment sense is one way, another is sector specific.

I have been approached by some folks asking about how they could go about profiling OpenID Connect for particular vertical segments of industry so there's definitely that.

I can tell you that from my research into API management platforms where OAuth is pretty much the incumbent solution for API security and access control, OAuth 2 and various very popular profiles of OAuth 2 are supported as button clicks in the admin consoles of pretty much all the tools that we've looked at. So it's getting to the point where it's more routine but yes profiling is absolutely needed and some profiling has been done.

John Bradley – Senior Technical Architect – Ping Identity

This is John Bradley I'll add on slightly. So, there is some profiling work of at least OpenID Connect happening at the Federation Interoperability Workgroup at Kantara based on some initial work done by the GSA on profiling Connect and/or OAuth.

There are some general guides including a security consideration as part of the OAuth specification, but like TLS it's hard to come up with a specific profile without necessarily knowing what it is you're attempting to protect because the actual API and the environment that it's in may have very different considerations.

So, if you're trying to do a JavaScript application in a browser, the security considerations for OAuth are going to be very different from server to server communications. So, you really do need to take into account the environment the profile and the API that the profile is going to be protecting. So, yes there is more specific work that needs to be done certainly around different health APIs.

George Fletcher – Chief Architect, Identity Services – AOL, Inc.

And this is George Fletcher just one quick thing I'd add is OAuth 2 so far has not really been used in what I will call federated authorization sharing of tokens between different relying parties and I think that in and of itself needs more specification and maybe profiling but has the opportunity to significantly reduce user experience issues going forward.

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

This is David, just following up on that and from anyone that might have been left around from the first set of presenters that we had. Is there any focused effort on creating healthcare appropriate profiles for these standards that you are aware of such as from the IDESG or other groups?

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

This is Tom Sullivan. We have not discussed this in depth but we're hoping that the rest of IDESG will bring healthcare into this and bring us up to speed.

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

Thanks.

John Bradley – Senior Technical Architect – Ping Identity

This is John Bradley again, as part of the pilots certainly people have asked about general profiles but nothing specific about the development of general profiles for OpenID Connect which a large number of the pilots are using which is one of the reasons why the Federation Interoperability Workgroup is undertaking the task but there isn't anything happening that's specific to health.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

And this is Jeremy just to jump in, I think one of, you know, our goals for the pilots, you know, the pilots are, you know, essentially piloting new things that haven't generally been done in the marketplace before either with new deployments of technologies, new applications of standards or, you know, new use cases.

You know one of the things that we expect to emerge from the pilots and in fact already is starting to emerge as new technologies are out there is, you know, we'll develop a new set of requirements from those that starts to point to where we need either new profiles of standards or, you know, perhaps new standards entirely to support some of the new technologies or approaches that are being deployed.

But, I think at this point, you know, essentially being about 18 months, you know, into the pilots, you know, what you'll learn I think from, you know, the pilots panel that comes after this is, you know, you'll get sort of a mid-course or, you know, mid project, you know, assessment of where things are going and where they've been but I'm not quite sure that we're at the point where we're going to be pointing to, you know, sort of new standards deliverables at this point.

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

This is Peter Brown I'll just add one other thing to Jeremy's – is that the nature of IDESG is to try and build a framework of standards, policies, processes within a future framework and it may be, it may well be that it's not sufficient just to identify or to have established new standards, it may need to be complemented by aspects of public policy or in terms of recommended processes and procedures that partners ought to take forward.

So, I think it's always important to take a big picture. I mean, there are, you know, many of us involved in standards work say, you know, we love standards so much that's why there's so many of them. The issue is that, you know, when we take a purely standards-based approach we always think that we can solve the problem or a core problem just by having a clearer standard and I think it's important to inject an element of caution, a note of caution given the fact that it may not be sufficient to just have a standards-based approach.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Yeah, this is Jeremy, just, you know, one additional comment, I think most of the challenges that, you know, that IDESG is looking at is actually less around do we have, you know, good enough standards to actually meet the goals of NSTIC and more what are the policies and the business rules that are going to govern the use of these solutions.

I think the technology on the standard side, not to say that it's easy, but it is easier than some of the broader, you know, policy and business questions that need to get settled. You know I thought John Bradley made a great point earlier when, I think, you know, to paraphrase what he said, you know, there are not NSTIC standards emerging per se.

You know the steering group has a standards coordination committee that's, you know, looking at different standards that are out there and looking for where additional work may be needed, but, you know, with or without NSTIC the marketplace, you know, has been moving forward and will continue to move forward and coming up with better standards.

You know if we can claim credit for anything from our program it's that, you know, by throwing down a marker that, you know, points out we need better solutions that are secure, resilient, interoperable, privacy-enhancing, easy to use it at least can help to influence, you know, standards discussions, you know, worldwide, you know, to essentially reinforce that these are all important things that are out there.

But, you know, as John said a lot is happening outside of anything that the steering group is trying to do. You know our efforts at the end of the day are to catalyze the marketplace and when we see the marketplace coming up with better standards-based solutions we're quite excited on our end.

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

This is David, I appreciate those comments. I will make one declaration of one effort to create healthcare specific profiles, and I think it was briefly touched on by Eve in her presentation, which is the Blue Button Pull work done under the coordination of the S&I Framework at ONC.

The Blue Button Pull has not been a heavily resourced project but they have put together some OAuth 2 based, OpenID Connect, OAuth 2 based profiles for healthcare based in large measure on the MITRE work with RHEX, but it is standing out there needing validation from a broader group of people.

We are interested in using it at my company to build a framework for portable Apps in a vendor neutral way. We need to solve this problem if we will achieve any kind of plug-and-play. So, I will just register that there is a start out there but it certainly needs more validation.

John Bradley – Senior Technical Architect – Ping Identity

So, this is John Bradley – .

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

This is Michelle.

John Bradley – Senior Technical Architect – Ping Identity

From the panel again, just –

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

I'm sorry, can I interject, I'm sorry we are running very behind schedule and we have a lot of questions. So, I just want to make sure that we have the opportunity for other people to ask questions.

John Bradley – Senior Technical Architect – Ping Identity

Okay, just a quick –

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

Sorry about that. Peter Kaufman?

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

Thanks, this is simpler stuff, we're talking about NIST defined levels of assurance to assign identity and multifactor authentication but many systems are going to utilize a password as one of these factors. Passwords are pretty simple and straightforward.

I've seen on websites regarding password security that long passwords without requiring multiple character types are far more secure than shorter complex passwords. And I've seen the complex passwords, especially with frequent changes required are often written down compromising the local security.

Are there any studies looking into this and could that drive the industry to using longer less complex password requirements? I know this is kind of different than the stuff we're talking about but it's heavily involved.

Eve Maler – Principal Analyst – Forrester Research

This is Eve perhaps I can comment. I've just recently published a series of authentication market overviews through Forrester and the IAM systems of the world generally are very sclerotic in their understanding of what makes a strong password or a password with high entropy or good bit strength or whatever and so unfortunately that tends to make password policies easily settable that are not particularly helpful to security nor to memorability of the password so they sort of fail on all accounts.

There is some evidence, although it is disputed, that the sort of correct horse battery staple style of password, which I think you're sort of suggesting with a longer, you know, normal character passwords, there is some more friendliness to that that I see in the market.

Of course there is also slightly increasing friendliness to consumers at large but only slightly for stronger authentication methods that for example combine, you know, other factors that mean that the user has to go through a ceremony that's more complex.

Of course any federated model that is only based on password security, even if a relatively strong password, has some weaknesses and a single point of failure and of course federation and strong authentication of various sorts go nicely together.

I do not currently see a generalized move towards improving how we get password strength except as it relates to real-time password strength checkers displayed to users when they set their passwords.

George Fletcher – Chief Architect, Identity Services – AOL, Inc.

One, this is George Fletcher, one other comment is often times when it comes to attacks and compromise the issue is not so much the strength of the password but the diversity of that password within the context of the overall set of users because the attackers – I mean we tend to be creatures of habit and also as attackers look at the passwords that do get expose they find the patterns that are common across us as individuals and then they leverage that.

So, even those, the four, you know, five letter words while maybe even higher entropy, right, can still fall into common patterns based on just the fact that were humans and we do things in similar ways and think in similar processes. So, I don't know that overall that's going to be a significant increase in security of the identity.

John Bradley – Senior Technical Architect – Ping Identity

So, John Bradley, just quickly there is almost no way to fix passwords. There are interesting – there is interesting proprietary information that the various large ISPs have about what the account breach – the password forcing activity is and its quite interesting being able to actually see in real-time what passwords are being tested against accounts for compromise.

The other thing that people are starting to do, and is being recommended by some people, is password managers which if you think about it now introduces yet another potentially unsupervised unaccountable mechanism for – that people may, you know, rely on some password manager provided by someone in the Russian Republic, what have you, were you may actually start – as people start using password managers to manage the complexity of passwords we may start losing passwords out the back door through the actual password managers, because they tend not to be supervised in any way.

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

Yeah, this is Peter I'd just echo the last two comments. I mean, the – I think the issue of password strength or complexity is at best a Band-Aid on the system.

If you look at the development of network computing infrastructure over its history of the last 60 years the user ID password paradigm I think is the only and last remaining part of the initial infrastructure that was set up in the early 1960s. So we're far away from being able to deal with this issue.

The strength of brute force attacks and the power that brute force attacks are just so far out there today compared with what was expected not to be a situation 50 years ago.

But it's the paradigm that hasn't changed and I think Jeremy was right in highlighting, you know, the high percentage of 75% of compromises being a result of attacks on passwords.

So, I think it's a – I think it's a futile exercise in the long-term in trying to just make passwords more complex. I think we just have to change the paradigm in terms of overall authentication and identification issues.

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

Well that wasn't what I was talking about I was referring to passwords as a second factor, they're still going to be utilized in two factor authentication in a lot of systems and password strength is still important but the answers were very helpful, thanks a lot.

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

Thank you. Wes Rishel?

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

Thanks, Eve, just at the very end of your testimony when Michelle just about had the hook wrapped about your neck to drag you off you mentioned something about expanding on the credit card liability shift model as apparently as something that we want to consider. I wanted to give you a chance to maybe spend another minute or two explaining what that was about?

Eve Maler – Principal Analyst – Forrester Research

Okay, this is Eve responding, thank you for that opportunity. I'm not sure exactly where it would go but I was fascinated to learn about the liability shift that essentially the trust frameworks of the US credit card industry have implemented in moving to the EMV model, to the chip in the card model.

And what they're doing is they recognize that they have multiple distributed parties so you essentially have merchants that are kind of relying parties and you have the credit card issuers that are the – kind of like the equivalent of an identity provider and you're going to have in this very, very large ecosystem differential deployment of technology, credit card issuers that haven't quite got their act together as fast as some of their competitors in terms of sourcing the cards, getting the cards out and so on and merchants that haven't deployed the new readers.

And so what they've done is say, if you're the weak link in the chain you except, by virtue of participating in this ecosystem proportionally more liability, so it incentivizes a race to the top in terms of turning over your technology to get to a stronger basis but it doesn't require you to and you can make a business decision.

So, I think it's a really interesting exemplar of solving problems of liability in loosely coupled systems with partners of differential sizes and capabilities that may help us understand how IdPs don't have to necessarily take on all of the liability for issuing a strong assertion, which is what we're trying to get them to do and for, you know, decades now almost we've said thanks and Telcos have been natural centers of where that could be done, but in many, many cases certainly in the US we don't see them rushing to do so and those rushing to be accepted. So, I thought that it might be worthwhile looking at that example to say what lessons can we draw?

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

And so, I think that one of the characters for the financial industry is that they have a clear monetary assessment of risk or of loss not so clear in the healthcare industry.

Do you think there's a way to adapt that model to an area where you just don't have this liquid pool of money you can divide up according to proportional blame?

Eve Maler – Principal Analyst – Forrester Research

You know, you're right, I mean, the analogy is clearly not perfect and I mostly meant to try and be provocative or evocative or something.

But, I have noticed that in this new era in the US where the EHR suppliers are – they're getting their systems rolled out in a lot of new practices and hospitals, and institutions and I myself, just in the last few weeks, you know, created two logins at different EHR systems which are clearly deployed as multitenant fast systems that multiple practice can have a sub-domain in, and what that taught me was that in a healthcare ecosystem right now if I had to bet on who would be the IdP and who would struggle most with the question of liability and strength of log it would be those EHR providers.

And there is kind of like, you know, maybe the big six who own most of the market and a whole bunch of others, so it looks a little bit like social login, you know, there's only 20 or 30 IEPs in the world that the vendors in that space have found valuable to integrate with.

So, it reminds me of that and it makes me think that there is an interesting opportunity/risk for those EHR vendors that already have patients creating logins at them and have the capability to attach those patients to multiple tenants that they have, multiple customers that they serve with the records, but may be very wary of doing so. So, that's just a few thoughts and I don't want to go too much longer and save it for the other panel.

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

Well, thank you it helped me understand what you're about, very helpful, thanks.

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

Michelle, do we have any others?

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

We have lots of others so I'm not sure how we want to do this, well, two others, Dixie Baker and Leslie Kelly Hall. So maybe we can be very quick and then move onto our next panel.

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

Thank you.

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

Yes, go ahead.

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

Thank you for asking. Thank you for – this is Dixie Baker. Wes, thank you for asking that question and Eve thanks for the answer that was really interesting. My question may best be directed to Peter.

I'm involved in an international healthcare effort and so I am acutely aware of the differences in the perception of trust between jurisdictions and in some cases these differences are actually openly acknowledged in law itself.

And I think we have a similar situation in the US among the states and among provider organizations where they just don't necessarily trust each other.

How do the NSTIC concepts and standards, and the policies that you've mentioned, all of you have mentioned, address or accommodate these differences in the perceptions of trust?

Do their need to be multiple levels of strength of assurance in the credentials issued or how is that accommodated?

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

I mean, I don't want to be too philosophical in my response, but I think the key lessons we've had so far is firstly and several people have referred to this already that, you know, one-size-fits-all or one-solution-fits-all is certainly not an approach.

I think a classic example of where that is problematic is in the area of health ID theft something I've been working on with the Attorney General's Office here in the State of California. For example, healthcare providers may write down medical ID theft or rather insurers, healthcare insurers may write down the issue of medical ID theft as just an economic cost of operation that there's a danger that somebody takes somebody else's identity because they're not insured and they want to benefit from somebody else's healthcare plan. It's a known risk, it's a known factor and something that health insurers generally tend to deal with as purely as an economic cost.

However, from the point-of-view of contamination of health records it's more than just an economic cost, it could be a question of life or death if somebody pretending to be somebody else, their diagnostic information is added to what then becomes a contaminated health record, it's not just a health – it's not just an economic cost to the insurer it's a major issue for the healthcare provider, for the practitioners and for the original patient themselves that there is news that their medical ID was compromised.

And I think this highlights for me, it's an example which highlights the issue what you mean by trust and who you are trusting. And I think the only answer I can give in the general terms to your question is that the development of a trust framework or some sort of combination of trust marks or various other trusted parties within a future identity ecosystem will necessarily have to be taken into different factors which are not just economic, not just personal, but also look at these various issues with regard to the impact of trust or lack of trust from the different parties.

And I think the final comment is that trust is very much a human concept, systems may be trustworthy, they may be worthy of our trust, they may be reliable, they may be secure, but ultimately the issue of trust comes down to the human being in the loop and I think that's something which we're acutely aware of in the work that we're doing within IDESG and something which is very difficult to get their heads around in terms of coming up with tractable solutions.

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

But it's not always just a, you know, especially international, the US is not trusted as an entity, and it's not just a human as well, so credentials issued in the US are likely to be less trusted than those issued elsewhere.

Peter Brown – Identity Ecosystem Steering Group (IDESG) – Independent Consultant

Well, they may be trusted but again in a particular context do I trust that this person is insured for a particular type of treatment, maybe, do I trust that this really is the person who they say they are and they're in an emergency room then I may have to take on trust what's said even if I don't have a high level of assurance because I have an immediate duty of care.

If it's a question of for example, to take my own example, you know, of being insured in Belgium but a resident here in the United States, the ability of healthcare providers here to trust my credential as being who I say I am, but also to be able to trust and even access the healthcare records that may be held by multiple providers in the countries, you know, the sort of long trail of places that I've lived over the last years becomes a very difficult and very intractable issue to deal with.

And ultimately it is the healthcare practitioner face-to-face with me as a patient which is still the principal vector of trust in those sort of cross border relations, I wish it were otherwise, but I think that's the reality today.

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

Thank you, Michelle, can we go to the last question and then we'll end this panel?

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

Sure, Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Hi, yes, on full disclosure I am a member of the DirectTrust Board of Directors but I wondered if there is discussion between the work that you're doing and the emerging trusted frameworks that have been in Direct as required in the current Meaningful Use standards, the use of Direct but in DirectTrust per se for that trusted framework? Has there been any discussion between these groups?

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

This is Tom Sullivan, David Kibbe, are you referring to DirectTrust.org?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I am.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

So, David Kibbe was the Vice Chair of our committee for the first few months and I think there is another person Scott Mace maybe who are involved with DirectTrust and do attend some of the meetings. So, they're aware of what's going on from the Healthcare Committee's perspective but other than that we haven't had lot of collaboration.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you.

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

Okay, I think, this is Walter, I think this is a good time to end this panel. I do want to thank, this was a really great panel, thank everyone especially Nat who joined us from Japan, so thank you so much Nat for joining us. And I think with that I'm going to turn it to Dixie. I think we are scheduled for a break, but we can certainly adjust some of the time that is coming up given, you know, we're off about 10 minutes or so. So, Dixie?

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

Yeah, I think we owe people a break, we have scheduled a 10 minute break perhaps we should reduce that to 5 minutes is that reasonable for everyone? Michelle is that something that we could do?

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

I have 12:12 Eastern Time, shall we do 7 minutes, and come back at 12:20?

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

Sounds good.

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

All right.

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

Sounds good, okay, thank you.

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

Thank you.

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

All right we'll be back at 12:20 then, thanks.

M

Thank you.

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

And people don't need to hang up or anything we'll just leave lines open, thank you.

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

This is Michelle, I have 12:20 on my clock, do we have Walter and Dixie back yet?

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

Yes, I'm here.

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

Hi Walter.

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

I am too.

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

Okay, so I think we're ready to get started again.

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

Okay, sounds good. So, is the line open at this time?

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

Yes, we're still open.

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

All right, welcome back everyone, our next panel is actually we're going to start talking about real implementations of what we've been hearing about the NSTIC and the standards that NSTIC is looking at and the ecosystem that has been developed around the use of this common identity.

We're going to hear from three different pilots, Jeremy mentioned that there were, I believe he said, 12 pilots underway and we're going today to hear about three of them, the first, in the first presentation Cathy Tilton will be talking about a pilot that is being done around the provision of secure access to customer applications that's being offered by the AARP and Cathy is from Daon.

Secondly, we'll hear about the cross sector digital identity initiative, CSDII and this one will be – the testimony will be given by Michael Farnsworth who is the Program Manager for this CSDII Initiative, that pilot is being led by the American Association of Motor Vehicles.

And then finally, we'll hear from Douglas Glair who is the manager of the digital partnerships and alliances at the US Postal Service and he will talk about the Federal Cloud Credential Exchange Program. So, with that let me call upon Cathy Tilton.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

Thank you, I do want to say that even though we are behind schedule I am going to take my full 10 minutes because we have lots of lessons learned on our pilot. So, with that good day, my name is Cathy Tilton and I lead Daon's NSTIC pilot which we called, advancing commercial participation in the NSTIC ecosystem.

Our pilot is funded as a cooperative agreement through NIST and began on 1 October 2012. A full disclosure I also Chair the Standards Coordination Committee of the IDESG so was very interested in the earlier remarks.

Daon's NSTIC pilot employs strong risk-based multifactor authentication using a mobile device platform. This technology forms the basis for a new innovative identity provider service in which relying parties can dynamically choose the level of assurance needed for a given transaction and the particular authentication challenges to be issued to the device including biometric options.

Our pilot intends to investigate five primary areas, first the suitability of strong mobile-based authentication technology including biometrics for online authentication, the willingness of our piece to move to external identity and credential providers and how this fits within their business models, the acceptance of subscribers, the capability of existing trust frameworks and certification schemes to support these scenarios and technology, and lastly, the degree of interoperability achievable.

To answer these questions we plan to align our TrustX IdP with existing trust framework standards and NSTIC guiding principles, have this service certified for a level of assurance 3 and pilot it with five cross sector RPs while in parallel embarking on a research agenda with our partner, Purdue University, to assess and identify improvements in the areas of usability, accessibility, security and privacy.

The most notable relying party participating in our pilot, as mentioned, was AARP. And AARP's goals for their pilot participation are to improve their members online experience, facilitate new services requiring higher levels of identity assurance, protect member information, reduce the number of individual identity credentials required, give more control to the individual member, support family and intergenerational applications and this gets to delegation of authority, and investigate usability and user acceptance.

So, in selecting a use case we first had to identify applications where higher levels of identity assurance were warranted as many existing AARP member services do not require this. AARP selected, as their first use case, access to the AARP health record, which is a personal health record service which is free to all AARP members and which is an easy to use online tool designed to help people over 50 manage their family healthcare needs.

It lets them safely store and access critical health information such as medication, allergies, blood type, immunizations and emergency and provider contact information, lets them print an easy to read pocket card with vital stats.

They can also quickly access their health information from any computer, mobile phone or tablet and helps them prepare for emergencies by allowing them to store their family's health information in one easy to access location.

As the information stored in the AARP health record is very personal and sensitive access to the PHR becomes a transaction of consequence warranting higher levels of protection and a password. At present we are in the process of integrating the AARP application with the TrustX IdP with the first phase of the pilot anticipated to go live in the June timeframe.

Because we're introducing an innovative solution we have been pushing the envelope in a number of ways that are bound to uncover challenges, we expected to identify gaps in the status quo and we have thus we have no shortage of lessons learned along the way and I'd like to share a few of those with you today.

So, the first to challenge we ran into involves the identity model itself. Remember we started this about a year and a half ago. Existing trust frameworks were built around what I'll call a full function IdP that

is one that encompasses the functions of registration authority, identity repository, credential provider/manager, and credential verifier where the authentication is performed.

However, we found that many RPs have an existing base of subscribers that they already have a relationship with and for which they possess identity data. So, they have no need or desire for us to replicate the registration authority function but are only looking for strong authentication credentials that they can then bind to that identity that they hold. So, this aligned well with our existing identity X platform capabilities.

However, this credential manager or token manager component service was not certifiable under the existing schemes even though it was evident that there was a market for it. So, as a result we were forced to build out a full IdP service because we had no guarantee that our component service could be certified.

However, the good news is that the trust frameworks have since moved in this direction and FICAM has issued the new TFPAP the embraces the component type model which you heard about from Anil a little earlier.

This also supports a broader marketplace where IdPs can be created from what I'll call pre-certified components though of course the IdP itself must still be certified and service providers can concentrate on their area of expertise.

The second challenge we encountered was that existing standards are not necessarily innovation friendly. NIST SP 800-63 is very prescriptive in its definition of token types and although the concept of equivalent and comparable methods exist the process for determining comparability is undefined.

So, we, in our case offer methods that are equivalent to the multifactor software crypto token, however, the implementation on a mobile device differs from that prescribed in the standard.

So in a white paper we compared these methods including a comparison of token threats and showed how our method was equivalent or better than the described implementation. Government reviewers agreed, however, because no process of declaring equivalence exists, we were stuck.

So, the only way we could move forward was to submit a change request to SP 800-63 and that's, as you know a very lengthy process. So, we actually wrote our first paper and began discussions on this issue in February of 2013 and we're still in limbo on this issue.

Related to the above are gaps related to dynamic risk-based multifactor authentication and biometrics and we ran into the following standards gaps. First of all SP 800-63 does not recognize biometrics as a token type even when restricted to a second or third factor and the SAML authentication context option does not include a code for biometrics.

Second, the ability of RPs to dynamically select authentication methods is limited. In some cases the RP may request and authentication at a specific level of assurance which can in turn be mapped to a set of methods but this restricts the number of combinations available.

Some functions must be performed administratively rather than dynamically for example policy management, queries for registered or bound subscribers and blocking or unblocking, or unbinding of subscribers.

Also, authentication requests do not allow for setting of geolocation boundaries, transaction descriptions may not be passed to the IdP for display on the phone therefore these must be administratively set and so this limitation is actually good for privacy but not as good for security or troubleshooting.

Ascertains may not contain additional contextual information, for example in some cases the return of biometric scores which might be useful. And there is lack of – capability particularly between the RP and the IdP.

So, our fourth challenge that we confronted was FIPS-140 Certification of Cryptographic Modules on Mobile Devices. So, although all four major mobile operating systems, IOS, Android, Blackberry and Windows have received FIPS-140 Certification that certification is very specific to the dot release of the operating system and the chips that test it. Not every possible configuration is on the certified products list.

Worse, when a new OS version is released a certified device instantly becomes an uncertified device. When the mobile device is used as the authentication platform the issue becomes apparent. However, these same platforms are used for mobile banking every day.

In SP also – in SP 800-63 for example a password or SMS token are given the same level of assurance as a single factor crypto token, LoA 2, however there are no certifications required for these methods. Also commercial entities trust TLS provided within browsers and mobile platforms so it's not unreasonable for this to be accepted by trust frameworks as well.

Our fifth challenge, we also found multiple standards gaps in the areas of sponsorship and binding processes and interfacing to identity proofers and attribute providers. Existing standards also appear to be biased towards the issuance of credentials in the form of heart or physical tokens and secrets, and standard interfaces and profiles are not targeted to in-band applications which creates problems for RPs developing mobile applications and wanting to incorporate trust framework compliant credentials.

Number six, standards do not always considered that someone has to pay but are more geared towards the free model which may be appropriate for the lower levels of assurance but not LoA 3. Business models need functionality for payment and reconciliation purposes for example, binding of subscribers has another purpose beyond security, the RP is in fact agreeing to pay for that subscriber to use the credential as their site.

We implemented both SAML and OpenID Connect and face challenges in creating a common user experience for both. I should say the reason we did that is so that we could interface the RPs that would choose one or the other of those standards.

Most notably OpenID Connect allows the RP to request user attributes on a transaction basis whereas SAML requires this to be done once when the RP IdP relationship is established. We also discovered that although OpenID Connect is becoming popular for commercial applications it is too bleeding edge for some RPs including the government.

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

Thirty seconds.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

Lastly, we found that both interoperability and privacy come with a price. Implementing privacy enhancements can come at the expense of some business processes such as troubleshooting, customer support, lifecycle functions and payment reconciliation.

And some interesting predicaments arise when issuing interoperable credentials such as the case of revocation, what happens when one RP blocks or unbinds a subscriber when and how should this be handled with respect to other RPs who have bound to the same subscriber? If the reason is that the subscriber was found to have falsified their identity or committed fraud what is the IdP's responsibility and will the IdP even know the reason?

Time does not permit me to provide a more comprehensive list or additional details but I'm happy to answer your questions during the discussion period. Thank you very much for your attention. I'm honored to have been asked to address you, thank you.

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

Thank you very much Cathy we appreciate your testimony. The second pilot being – the second speaker is Michael Farnsworth.

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

Yes, hi, how are you this is Mike, I believe I had a set of slides I was going to kind of walk through, if we don't find them maybe go to the next one and thank you and I'll work to try to keep my remarks brief so we can honor the agenda for the other presenters that are following behind me. I know we have a lot of information we've gathered over the last 18 months so digesting it into 10 minutes has been a little challenging.

First, I want to thank you for allowing me to testify today on our pilot activities, as you know my name is Mike Farnsworth and I have the honor of leading the Cross Sector Digital Identity Initiative also known as CSDII NISTIC pilot. We are a public/private consortium of organizations and we came together really to explore putting stronger credentials in the hands of citizens by elevating the assurance of social credentials and to essentially make the Internet a safer place.

Our member organization include the American Association of Motor Vehicles, the Commonwealth of Virginia DMV, biometric signature ID, Computer Associates and Microsoft. We were actually part of the first round of pilots and are funded as a cooperative agreement through NIST and we also began on October 1, 2012. Can you go to the next slide please?

Our CSDII pilot really has three major components, our goal is actually to leverage an existing credential or token that's actually issued in the hands of the citizen by an existing identity provider, we also have mechanisms to issue other credentials but the basic premise was that we could take an existing credential or token that a user had access to such as their Google ID, their Facebook, their Live, their Twitter account and add a little bit more value to it by augmenting it with authoritative sources of information or attributes that that individual wishes to utilize in order to verify their information that they would present to a relying party.

It is important to note that the use of these sources is voluntary and is always initiated by the individual. CSDII is not an attribute exchange but we act on the behalf of the user who wishes to provide the information to the relying party.

The third component that we leverage is a valid identity proofing mechanism. These can either be an in person proofing event or it could be a remote proofing event. And we actually use a secure linking process to bind all this together so that the relying parties actually get a good consolidated representation of that individual and that kind of puts the necessary privacy controls in place. Next slide.

Our architecture is a cloud-based user centric model that allows the user to take a commercially available credential, whether it be a social credential or token, augment it with some verified attributes at the request of the user, couple that together with either a remote or an in person proofing event and then we memorialize and bind it together by introducing a second factor of authentication.

The end result of this is a stronger identity proof multifactor credential that's using components that the individual is already comfortable with. We traditionally don't do this today for high-risk transactions or sensitive environments due to privacy concerns of using federated credential and the chance of attribute promiscuity.

Our architecture actually removes this risk by isolating the participants and providing the necessary privacy controls for the information that is shared amongst the participants via our privacy enhancing technology provider.

Our PETP provides the necessary blinding between the participants to ensure that only the information the individual wishes to be presented is sent to the relying party and that the use of the credential is not subject to the linking and tracing of their activity.

By combining all the capabilities of identity providers, identity proofers, attribute verifiers, attribute providers, credential service providers and the privacy enhancing technology provider we're able to enforce the privacy controls between the participants and relying parties such as healthcare systems can utilize third-party credentials without exposing their systems to marketing and privacy issues. Next slide.

In order for us to effectively deliver the pilot over the two-year period we divided it into four core capabilities that utilize the three components in different fashions. Our strong authentication represents the verification of specific attributes for the pilot's purposes against the Department of Motor Vehicles authoritative data through the American Association of Motor Vehicle Administrators.

We then augmented the base credential with this unverified information that was provided by the users. While this isn't considered a proof credential it is more useful to the relying party to determine if an individual is who they say they are.

Our stronger authentication capability takes this base strong credential and adds additional assurance in the form of identity proofing and the introduction of additional tokens. Our stronger credential is the culmination of the two above and represents enrollment of the second factors and utilization of the in person proofing events with the multifactor authentication.

And finally, consolidating the asserted claims that are presented to the relying party and presenting them back with the confidence that the individual had utilized a combination of verification and authentication steps that provides sufficient assurance that the individual is who they say they are without exposing data or PII to other participants that aren't entitled to that information. This is where we essentially filter the attributes necessary for the relying party to make the authorization decision. And in our pilot we also use these attributes to associate federated credential with the electronic health record of our relying party participant.

All the while, while we are doing these four we are actually evolving our trust framework which encompasses the business, legal and technical aspects of the interaction and given our user centric approach, the user experience is always taken into consideration across all the capabilities in the implementation. Next slide, please.

Our first relying party participant is actually Inova Health System which is based out of North Virginia, and we're specifically tackling two use cases for them. The first one is patient access to their electronic health record utilizing a social identity provider, verifying attributes about the individual that they wish to be presented so we can associate to the appropriate record and the introduction of two factor authentication for them to actually access the portal.

The second use case that we are tackling for them is provider access to the health system, this not only includes access to the electronic health record but also to the health system network as several of the applications that providers traditionally need to access require access outside of the web portal.

A particular interest to Inova is the introduction of some strong identity proofing that goes into the issuance of the credential, the extension of multifactor authentication to non-network providers or those that have a business need in order to access clinical information but may not be part of the actual health care system. Next slide.

As you can imagine, you know, trying to actually implement this has – we have had several challenges and I'll kind of outline them here today. I've kind of put them in the order of, I don't want to use the term order of importance, but they were in order of invisibility.

You know I mentioned the trust framework earlier, one of things that by articulating our business, legal and technical controls we've actually established a trust framework mapping an analytic device that is actually being leveraged in the IDESG for how we can align the challenges and lessons that we learn in order to enable a trust framework provider to actually enforce the policy and the privacy claims.

The first thing that we actually had to address is some of the regulatory controls that are imposed on healthcare systems, we know that they are a very heavily regulated industry and there is a lot of controls that are put in place.

The first one was around protected patient demographic data usage, if information is provided by a patient in a healthcare system for seeking care can it be used for other purposes such as authentication whether it be a contact number or whether it be an e-mail address.

Aligning the use of a federated credential and the use of this information does it actually conform to HIPAA and are there additional controls that need to be introduced?

And then also the use of these federated credentials in order to enable the health care system to meet Meaningful Use and actually start to put more higher risk transactions on their web portal.

Another challenge that we actually had to address is the perception, the use of a social IdP or a social credential to access your health record has some stigmas attached to it when it comes to the potential for marketing and linking. You can imagine somebody accessing a test result that may show some different, you know, blood variables such as, you know, potential diabetes and then all of a sudden they're getting e-mails in their inbox around diabetes medicines and diabetes treatment, it probably wouldn't go over too well.

Also, moving out these federated credentials from the control of a health care system brings up the topics of the data breach and liability, all the while, while CSDII doesn't actually handle the PII as being provided by the individual, the perception of data breach and liability are some things that we have to take into account.

Additionally, there is internal and external views on the use of these credentials. The healthcare systems have a traditional model of, you know, issuing the credentials and so naturally there are a lot of questions about the usage of external ones. Next slide.

I believe Eve kind of mentioned, you know, in one of the previous panels integration with electronic healthcare record systems is sometimes challenging inserting additional capabilities and being able to do the associated binding between the identity and the patient record sometimes requires changes to the actual interfaces, network access blending a federated credential mechanism that has different steps in issuance of it not only to a web portal but actually to a network and then controlling that identity and how it's presented to the downstream systems within the network also brings in several different other challenges. Security protocols that are actually being utilized –

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

Michael, this is Michelle, I'm sorry –

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

Yes?

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

You are out of time but since I didn't give you your 30 second warning if you can just quickly wrap up.

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

Yes, absolutely. So, the use of more RESTful approaches and then of course the impact to the process flow and I think I only had one more slide, the last one.

So how does healthcare factor in? We know that healthcare industries really set the bar very high because of the sensitive information it really promotes a privacy lens and solution development in leveraging the PEM that was referenced early, it does trigger regulatory questions.

Putting in stronger identity proofing can streamline enrollment, it can augment existing mechanisms and then market adoption and consumer and patient education are two ways that healthcare systems can help by interacting with individuals, it's actually a good way to promote the use of strong credentials in sensitive transaction environments. Sorry, I know I ran over a little bit. I apologize.

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

Thank you very much Michael for your presentation and our third pilot that we'll hear from is the Federal Cloud Credential Exchange Program and our presenter is Douglas Glair.

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

Hello and thank you to the members of the committee for inviting me to talk about the Federal Cloud Credential Exchange. I lead up the US Postal Service focus on consumer identity services and the FCCX Project is one of the initiatives we are actively involved in, in partnership with NSTIC Program Office and GSA.

The Federal Cloud Credential Exchange is both a technology solution and an NSTIC Program helping to facilitate the government's early adoption of FICAM approved interoperable credentials. FCCX addresses the benefits for agencies, identity providers and most importantly the consumer which I'll address.

From a technology solution the postal service is the operating entity responsible for the FCCX hub. The technology hub enables reliant parties or agencies and FICAM approved identity providers a single interface point for access to each other. Let me elaborate on why this is a key benefits.

Agencies and identity providers could build independent interfaces and connect directly to each other using the FICAM approved profiles but this adds complexity, cost and time to the ecosystem. For example, if we had five agencies connected with five identity providers directly to each other that means we have 25 unique interfaces going back and forth a fairly inefficient process requiring independent building, testing and maintenance.

By integrating identity hubs such as FCCX we solve this by allowing each agency and identity provider to connect one time to the hub using approved profiles thus immediately reducing 25 interfaces down to 10.

The hub further simplifies the process for agencies as it automatically displays for the agency on their webpage through embedded selector the available identity providers meeting their specified level of assurance and identity attributes that they are requiring from the identity providers.

As new identity providers are added they automatically become available to the agencies on their webpage and vice versa as more agencies are added and participate the identity providers have instant access to those agencies.

We leverage standard FICAM profiles, integration with the agencies are done through SAML 2.0, FICAM approved profile and we also handle that same integration for credential or identity providers for level 2 and above. We are integrated and OpenID Connect LoA 1 identity providers here in April.

The FCCX hub also benefits citizens by protecting their privacy, the hub blinds the identity providers from knowing which reliant party the consumer is trying to log into and the hub additionally blinds the reliant party from knowing what identity provider is used. This addresses the concern of can my rise in Google, PayPal identity providers see where I'm interacting across the federal government. We do this by managing the meaningless but unique identifiers within the system but never storing any personal information within the FCCX hub.

USPS role as operating the operating entity to the hub included the competitive solicitation and selection of the technology solution, and the ongoing management of that solution, the hub is completing the FedRAMP certification for security reviews in addition to postal's own security reviews and certifications.

We are leveraging a FedRAMP approved hosting provider and USPS is also backing the solution through our own office of secure – Information Security Office and the US Postal Inspection Service. We take the security and protection very seriously for all of these applications and this is one of the reasons that the postal service has been named the most trusted government agency for 7 years in a row.

Moving from FCCX as a technology hub to the overall NTSIC Program, as was described earlier, it's a joint effort between NSTIC, GSA, the Postal Service and the agencies that are participating and a key financial benefit to the agencies of leveraging this program is then all agencies are able to pay for credentialing as a service or authentication as a service one-time and pool those capabilities versus each independently paying directly to each identity provider.

Basically, the model will be that there is unlimited usage per credential on an annual basis were all agencies are able to leverage those credentials for one price for the year. The more agencies that participate the overall lower total cost to the federal government versus them each independently paying.

The FCCX Program is also developing recommendations for agencies display and messaging of the interoperable credential partner use to help move citizens from using proprietary individual credentials to an interoperable one.

In summary, FCCX is about enabling consumer choice of credentials that they can use across federal agencies while ensuring the consumer security and privacy. The easiest and most cost-effective way for agencies and the healthcare industry to move towards interoperable credential use is through an FCCX like model so that it's a pooled set of resources and capabilities versus each independently trying to address it. Thank you very much.

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

Thank you, thank you very much. Okay, Michelle why don't we start the Q&A please?

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

Sorry, it took me a second to get off of mute. I don't see any questions – Wes Rishel has a question.

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

Thanks, this is to all the panelists and it's a kind of a general question and it has to do with our – how we should assess pilots in deciding on the readiness of a standard or a framework or something else to be rolled out on a semi-voluntary basis across the whole healthcare industry.

The pilots we're hearing about today seem to be very substantial, we have heard of other pilots that were less ambitious in their goals and what we're hearing is there are lessons coming in even before "go live." So, it's easy to understand how a pilot can show us what get needs yet to be done.

How can we assess a pilot to say it shows there is not anything left to be done that it's now ready for primetime or that there is a clear list of issues and if those are solved it's ready for primetime? Thanks.

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

This is Mike and I may take a quick stab and then let Doug and Cathy kind of follow into it and, you know, you heard me reference some of the work around the trust framework and what that means, you know, part of one thing that we've started to introduce into the IDESG through the TFTM Committee is how to utilize an analytic device to essentially highlight what those gaps are.

You know walking through each of the business, the legal, the technical which span across the regulation to really come up with what are those areas that require attention in order for somebody to sign on.

One of the things that our pilot has been pushing over about the last six months is really trying to answer all those questions meaning, you know, having an independent privacy review from a third-party of those controls and of the technical implementation has been key.

And so perhaps, you know, leveraging something like these models that are coming out of the IDESG in these committees whether it be from the TFTM Committee, whether it be from the Healthcare Committee, you know, that Dr. Sullivan is leading, that these can kind of materialize into a tool that can inform what that maturity model looks like.

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

And this is Doug let me add on a little bit. From a pilot perspective I break this into two buckets, one is the decision of moving towards and leveraging interoperable credentials that's going to have a number of decisions that have to be made, level of assurance requirements, attribute requirements and those can be different even to reliant parties within the healthcare space. Adding a hub in the middle makes some of that significantly easier by having one place for each reliant party component and each credentialed provider to join in and connect.

So, I think each pilot is going to show successes. Is any one of them going to be a perfect pickup and implement without having to do and evaluate the exact needs "no" but I think you're seeing lessons and experiences on both sides interoperable credentials and hubs that need to be taken into account that will make life much easier for you long-term.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

Hi, this is Cathy, since I, think, gave the laundry list there of lessons learned I should probably comment. I think that the issues that we ran into were primarily because we were, like I said, pushing the envelope where we are looking for that higher assurance, we're looking to leverage, you know, mobile devices and we're introducing new methods.

So, it really – I guess I'd agree with Doug that depending on what it is you're really trying to do it could influence a lot, you know, how you would wind up using each of those standards and in what capacity. So, I guess that's what I would say.

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

Yeah, so let me suggest some things that I've thought of that might be helpful in our evaluating this question of when is enough, piloting enough. One is pilots that should most impact our decisions are the ones that have gone into production and are used for more than just a few test users.

Two they should involve interoperability across a number of organizations, a number of comparable stakeholders and three the pilot effort or the pilot report should include some instrument for evaluating the experience of the users and the belief that the user needs are being met. Do those sound like reasonable things we should be considering?

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

This is a Jeremy, I would say so, although I would say it is still worth considering some pilots that are a little bit more on the leading edge if only for that they're lessons learned both in terms of where they've had successes as well as where they've had challenges.

I think, you know, certainly to contrast, you know, Daon and FCCX, FCCX is really while it's a pilot, it's really set up as, you know, the initial iteration of what is expected to be a government-wide shared service that, you know, agencies are going to be using for live transactions really very shortly.

So, it's something that I think was arguably, I don't want to say less ambitious, but it was sort of designed, you know, as less of a stretch and perhaps some of the, you know, commercially focused pilots that our office has chosen to fund.

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

Yeah, let me just say I didn't mean to imply that each of these pilots is not very interesting and the presentations very helpful. I'm just sort of asking the stopping rule question rather than any means to deprecate – any intent to deprecate what's already gone on.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Oh, I wasn't suggesting deprecate, it was more, you know, one of our key tenets in our office is some pilots are going to struggle and that's okay, we learn as much from the pilots that have a hard time as those that are smashing successes.

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

Yeah, perhaps we should clarify that and Wes's question is really a good one. I've written down all three of your points. We have some metrics that we've developed, the HIT Standards Committee, has some metrics we've developed to judge the readiness of a particular standard to be considered as a potential national standard and part of that is maturity, part of that is implementability and Wes's question was aimed at getting toward, you know, how can we – where do we judge these with respect to fair value in terms of maturity and implementability.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

My apologies then I may have misinterpreted what he was saying. I would agree fully with you those are good criteria, yes.

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

Okay, thank you. Thank you for the question as well Wes. Are there other questions?

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

David McCallie has one.

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

Yeah, hi, it's David McCallie. This is – I'll start with Cathy but feel free anyone to comment and I'll try to ask it not in a negative way, but it's been my experience with a number of initiatives under the Meaningful Use Program where we've wrestled with trust frameworks that when you mix frameworks that would be adequate in the private sector with frameworks that are adequate for the government sector that the impedance mismatch can sometimes really make the problem awfully hard to solve.

And the government sector typically has higher levels of requirements and is more, I'll say, rigid or slow-moving of necessity, much more is at stake than the private sector where things happen more quickly and are willing to maybe take more experimental approaches like say OAuth 2 and OpenID Connect and more aggressively pursue them than say NIST is willing to support with their written specs.

So, Cathy your description of a year-long waiting process for approval of what sounds like a completely acceptable approach from the private side is what triggered my thought here.

So, the question is really, is it hopeless to try to get one size to fit all when we're talking about building these trust frameworks and we really should separate those two worlds and those people who need to live in both do so by choice or is it feasible to solve all these problems with a single unifying model?

M

Cathy?

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

Cathy are you on mute?

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

Oh, sorry, yes was, thank you.

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

I thought maybe I had stunned you with my question.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

No, no sorry I was talking to myself. So, I think that's a great question and I think we were very optimistic and trying to bite off cross sector implementations like that and I think that your question is particularly interesting when you talk about the government to citizen use case because that almost crosses the boundaries because you're talking about individuals who have mobile devices, who have browsers that are running on their machines and so that was where I saw the biggest disconnect was trying to take that into consideration.

When it comes to the other areas it's maybe a little less so but you pinpointed it, you know, in terms of the different considerations that the two factions have. I would hope that we could get there but it's a challenge.

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

Let me add to that, this is Doug, when I look what we're doing with the Federal Cloud Credential Exchange and that we are blending high levels of assurance all the way up to LoA 4 with cross federating with the federal bridge and PIV and CAC cards with LoA 1 requirements and needs for agencies, so I think the two can work together by leveraging a hub in the middle you're actually able to allow the agencies or reliant party to specifically identify, through their SAML request, this is the level of assurance I'm looking for, here's the specific identity attributes I need to know and the hub can then actually help the reliant party display only those that meet their criteria.

So, if in the future it's a requirement that you have to have two factor authentication and specific attributes the hub is only going to show LoA 3 providers that have those specific attributes that you're looking for.

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

Yeah I was going to say, and this is Mike, I was going to add to, I kind of agree with Doug's assessment and Cathy, you know, they actually do run at two different speeds and the interoperability and standards question is probably the first part that needs to be taken into consideration and then that's usually componentized and blended into the resulting trust framework.

One of the things that we had tackled as part of the pilot, given that we're a public/private partnership and we have state participation, state agency participation as well as the commercial sector, is making very sure that the trust framework components and modules, so to speak, are aligned appropriately so that they can be arranged in the right fashion for the participants to on-board.

One of the things that I didn't reference in my slide, but another thing that we're working on as part of this is the integration of this into the statewide HIE of which, you know, the Commonwealth has actually on-boarded onto, so there's a lot of synergistic opportunities that will come once we can kind of, you know, bridge together the different speeds, as you say, because you're right government speed runs on one track and commercial speed runs on the other and so trying to balance that is sometimes challenging but I definitely think that it's something that is actually workable and can actually be accomplished.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

And this is Jeremy, just to jump in, and I'll say I, you know, getting back to the question, I absolutely agree, you know, one of the questions that we got when NSTIC was first issued is, is this some sort of an attempt by the government to essentially try and push the government's rules, are they trying to push 800-63 and the FICAM certification process out to the private sector and the answer was absolutely not.

We actually, you know, recognized that there are some limitations and some challenges in terms of the way the government has approached this that may not necessarily be relevant to a lot of private sector use cases in terms of some of the solutions that the government has come up with and so, you know, I think one of the key challenge before the Identity Ecosystem Steering Group and really, you know, the broader market at large is, you know, can you come up with alternative frameworks for measuring risks, for establishing trust frameworks that are more relevant to the private sector than, you know, these four levels of assurance that the government has essentially defined and been building applications around.

One of the things I think we found is when you, you know, get 20 identity experts in a room from the private sector, you know, people are – it's really easy to pick a fight with the framework that's out there today. It's been harder to actually come up with alternatives and that's, you know, one of the things that the IDESG is really focused on right now is how can you take a bit of a different approach that may actually be easier for others to integrate with.

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

This is David, the original question here – I mean, just what triggered my question was Cathy's comment about specific operating systems dot releases on your cell phone. I mean, I would hate to think that the download I did last night to upgrade my iPhone to 7.1 would mean I couldn't log into my EHR the next morning because it was not approved through some, you know, federally mandated process that says each one has to be FICAM validated independently and the private sector would just not be able to tolerate that.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

I agree completely, so, and frankly it's something we struggle within the agencies too. I think, you know, a lot of our, you know, certainly when you look at, you know, the NIST special pubs that are out there and other things that agencies use under FISMA, you know, to manage their approach to IT security, you know, the fact that our computing environments continue to change and a lot of these were written when we were, you know, primarily using desktops and laptops and, you know, guess what I got a note from my security officer this morning saying don't upgrade your iPad or iPhone to 7.1 yet we've got to do some work on it still to make sure that it's okay.

You know when that happens, agencies – I would say NIST is, you know, being challenged right now to, you know, look at, you know, the way things are evolving and come up with, you know, new or better approaches to manage, you know, security and risk in light of them.

So, you know, again, this is why we would not necessarily try and point to, you know, something like 800-63 as something that you need to try and push out in the commercial healthcare space but then the question is, you know, what is the framework?

And I think, you know, our message is, you know, when you look at certainly, you know, the new body of standards that's starting to emerge and, you know, I thought Eve and others did a great overview of that earlier today and then look at some of the trust framework guidance that, you know, we expect to come out of the Identity Ecosystem Steering Group around a broader, you know, framework for identity over the next year that I think is where you may start to see some, you know, alternatives that, as this committee, as this Workgroup is considering what to recommend that ONC embrace you should have some broader commercial alternatives.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

This is Tom Sullivan, can I jump in here too with another comment?

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

Sure, yes Tom.

Thomas E. Sullivan, MD – Chief Privacy Officer, Chief Strategic Officer – DrFirst, Inc.

So, this whole discussion again highlights the importance of what Jeremy started out with the greater collaboration with especially some of the bigger players in the healthcare private sector but I would also emphasize more collaboration between and among government agencies.

You know healthcare is arguably the most regulated of all of the industries and I know the bankers and finance people would dispute that but I think those of you on this committee who are familiar with healthcare would agree it's pretty heavily regulated.

So, just example 800-63 it took a year for a couple of us to be able to show the authors that hospitals and healthcare institutions that signed the conditions of participation in Medicare – tremendous credentialing including LoA 3 and LoA 4, it took a year finally they were able to issue version 2 of 800-63 and they recognized that, you know, healthcare professional institutions as an example of that basically following the LoA levels.

So, I just would plead for ONC and this group to encourage more collaboration not just with the private healthcare sector players but also the different government agencies the DEA, AHRQ, you know, of course ONC is hosting and I think that's great but, you know, things like the FDA also that doing device identity which we've talked about in our health care committee also.

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

Thank you, Tom, thank you. Are there other questions Michelle?

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

This is Cathy could I just say one other thing, 800-63 not only is a – is intended for federal government but most of the existing trust frameworks depend on that standard and so a commercialized version of that I think would also be useful.

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

This is David –

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

Walter has a question.

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

I have another independent question if there are no other questions?

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

Walter has a question.

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

Okay.

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

Oh, yes, thank you. This is a really great conversation, thank you so much for sharing your experiences with the pilots and we heard a lot about different issues that you have found and it dawned on me that it might be helpful to hear what's your biggest, single biggest challenge that you found in your own pilots and how do you see it being addressed into the future?

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

This is Mike and I might, I mean if I was to summarize it, I think probably one of the biggest ones is the clarity of the regulations and the patterns that enable adoption of alternate mechanisms that are not embodied in current implementations, you know, if the goal is to shift to more user centric secure credentials that are outside of a participant's control, you know, they're subject to regulatory scrutiny on that and so by kind of adding a little bit more clarity and interpretation to that it really starts to help inform and promote the adoption.

One of the most valuable things that we had as part of the pilot that probably wouldn't have happened had we not had the support of NIST and ONC is actually gaining that clarity of the interpretation and the support of, you know, what we're promoting while it may not be 100% in line with say 800-63 it satisfies the regulatory, you know, controls that are in place and so I think that's probably a very valuable tool to kind of push these initiatives forward.

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

This is Doug. I can add from our project it's – as we've all been talking this is an emerging ecosystem that everybody is continuing to evolve. Agencies are evolving and realizing what they're going to need to map an identity to either an existing account and/or for somebody brand new coming and that's impacting some updates to FICAM that then has upstream impacts to credentialed providers and data they have to collect and/or manage.

So getting more of the parties all discussing these and making some – and being able to get in advance of what needs to be implemented to map an identity from a credentialed provider all the way to an agency and all the use cases we think we have tackled most of them but I'm sure there will be some more that will come out as we get through the first credentials flowing through the brokers. So I think everybody has to walk into it with an open eyesight set but also see that this is a better way to improve the security and convenience for the citizen.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

This is Cathy, our biggest challenge wasn't any of the ones that I mentioned, you know, I tried to concentrate on those that were standards related but our biggest challenge is really relying party adoption of external or federated identity particularly in the identification of high assurance use cases. So, that's probably the biggest issue.

Interestingly with regard to interoperability in the commercial sector when we talked to our relying parties about, hey, and you know, you're subscribers will be able to use this credential at other relying parties they didn't all think that was a great thing. In fact one of our relying parties said "well, why in the world would I want to enable my competition" you know so there are some perceptions there that hopefully the healthcare sector wouldn't be as impacted because I really see healthcare as a very, very good use case for a federated identity and maybe more open to the concept of external identity providers.

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

Thank you for that response all of you thank you.

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

Michelle are there others in the queue?

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

There are no more questions.

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

Then I have one question for Doug. I can certainly see the advantages of this identity hub but it seems to me that this would create a single point of failure and ideal target for a denial of service attack and I was wondering how you deal with that?

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

No, you're very right that all of a sudden by identities going through a single point of contact – that is why from a security perspective we're going through full FedRAMP review process making sure that we've got the capabilities in place that we have disaster recovery, we have fail overs in place to handle it.

And then as this evolves we actually may set up multiple nodes of the hub to actually handle a separation so that there's not a single point but that there are multiple ways to facilitate the authentication through different nodes of the hub.

So, that is something that we will continue to evolve through this and the last piece I'd clarify from a security perspective, the actual credential itself never transfers through the hub the credential username, password always stays at the credential provider.

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

Right, I was thinking more – I did understand that –

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

Yes.

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

I was thinking more from a denial of service perspective. Thank you.

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

Dixie, this is David, I have a hub question as well, do we have time?

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

Yes, please, yes.

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

Yeah, so I understand the values of the hub in particular to the degree that it is sort of like what we in healthcare would call an interface engine where it's kind of mapping between incompletely specified profiles but it seems like the existence – the need for the hub is just – I didn't hear any reason for the hub to be there other than that our protocols, our standards aren't good enough yet for the peer-to-peer connectivity.

In other words the hub sounds to me like sort of an Internet where you had to go to one place to get your web pages because we don't agree on how to do HTML. As soon as we agree on how to do HTML we wouldn't do it that way. Is that –

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

No, no not quite. Let me sort of re-clarify a little bit. So, the standards are there and the standards are very useable from a FICAM using SAML 2.0 FICAM profile agencies and credentialed providers could do that peer-to-peer integration today nothing is stopping that.

The challenge there is every agency then having to build and test every one of those interfaces the hub allows the agency to connect one time manage that and then as additional identity or credentialed providers come on they're able to automatically consume the service. So, it's actually a reduction of IT resources.

The second major component is from a costing perspective for the federal government being able to negotiate one set of basically contracts for identity as a service that all agencies can leverage versus every agency even if they have a master contract paying for that service directly to each credentialed provider.

And lastly, the hub adds significant privacy enhancing for the citizen that the credentialed provider does not know which agency the citizen is trying to log into actually addressing one of the big concerns by citizens of using an interoperable credential across the federal government.

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

Yeah that's – this is David again, that's an interesting point traded off against in this post Snowden era the lack of trust that's been created by the NSA revelations. So, I guess it's –

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

Exactly.

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

You win some you lose some.

Douglas Glair – Manager – Federal Cloud Credential Exchange Program (FCCX) - Digital Identity Services in Secure Digital Solutions Organization – US Postal Service

And that's the role also of the postal service being the operating entity to stand this up is we actually are the biggest federal agency touching citizens every day and being able to attest to them that, no we are – nobody is looking and seeing where you are logging into that if there is any type of forensic evidence that is needed that requires the Postal Inspection Service and actually cooperation across the agency, the hub and the credentialed provider to map all of those end buttons together.

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

Okay, Michelle, I think we're hitting up against another break, is that right?

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

We are, so Dixie, I'll defer to you, do you want to just take 10 minutes from where we are now?

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

Let's take until 1:30 how about?

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

Okay.

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

Yes, okay. Is that okay with you, Walter?

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

How many – which time zone are we in?

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

I was using the east coast time zone until 1:30.

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

Yeah.

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

What did I say 10:30 I meant 1:30. Okay.

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

Yes that will be fine. I'm hoping that Arien will be still available but if we need to switch him to be the first we can do that too, but I think he was going to be available, so moving it down, I think we're talking about 10 minutes from what we originally were planning I think.

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

No that would be – that would be consistent with what we originally planned.

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

Yes, exactly, thank you.

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

Okay, thank you, bye.

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

This is Michelle, do we have Walter and Dixie back? I have 1:30 Eastern Time.

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

Yes we do, I'm here and I think Walter is here as well.

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

Yes, I am here.

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

Yeah.

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

Okay, all right, so let's get started again.

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

Yeah, thank you. I'm going to be introducing our last panel, panel three and what wanted to do was, in order to conclude this hearing, bring together a panel of healthcare organizations that will provide their views and perspectives and experiences really with identity and access management and NSTIC. So, that's our intent with this panel.

And the panelists include Lisa Gallagher who is the Vice President of Technology Solutions at HIMSS and is actually also a member of the Health IT Standards Committee and this Workgroup.

Arien Malec who is the Vice President of Strategy at RelayHealth and a Lead Strategist of the CommonWell Health Alliance. I think Arien might not be able to stay all the way through the Q&A but David McCallie has agreed to step in to answer some of the questions that might come up regarding CommonWell Health Alliance perspective.

We also have Tim McKay who is a Principle Solutions Consultant with Kaiser Permanente's Digital Technology and Operations Group and he will provide Kaiser Permanente's perspective on identity management and NSTIC. He will be followed by Kevin Isbell who is the Senior Director of Health Information Exchange at Kaiser Permanente and the Program Manager for the Care Connectivity Consortium.

And then we'll hear from Mike Davis who is the Security Architect at Veterans Health Administration and also a member of our Workgroup here. So, that's our lineup but we'll start with Lisa, let me ask first, Arien would you have time right after Lisa or would you prefer to go first?

Arien Malec – Vice President Strategy & Product Marketing – RelayHealth Corporation

No, I have time until 11:00 so that would be fine.

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

Okay, so we can start with Lisa. Lisa, please go ahead. Lisa you might be on mute. Hello, Lisa?

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

So, maybe we should start with Arien.

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

Yeah, I think, okay we'll start with Arien and try to see if we can connect with Lisa, but Arien why don't you go ahead please.

Arien Malec – Vice President Strategy & Product Marketing – RelayHealth Corporation

Thank you so much and thank you for the introduction. As you know CommonWell Health Alliance is a developer led HIT led organization that's establishing patient matching, linking consent and authorization and data access services nationwide. And along the way we have tried to solve a number of interesting problems related to the identity of healthcare organizations, providers and patients.

And what I'd like to say in summary is that on the healthcare organization side for a number of reasons we believe that organizational identity is the most important and compelling attribute because HIPAA defines privacy and security at a covered entity level and because there are multiple roles in healthcare where extenders, proxies, staff perform roles and activities on behalf of an organization.

We believe it is most important to identify the legal organization and identify the relationship of that organization to the individuals, to do this we identify the organization based on a TLS certificate, another means and then we let that organization, through the use of SAML assertions, assert the role of the individual or other kinds of roles that's involved in a transaction as an example of other kinds of roles we have a number of use cases where a machine, such as an EHR is constructing a summary document on the basis of the most recent information that's available and in that case the responder is actually a computer that is responding on behalf of and dually delegated by the organization.

We believe that organizational identity that pattern of organizational identity as the key identifier and the key identity to manage in health information exchange and other functions has been borne out by other initiatives, the Direct Project for example, most of the uses of certificate and signing encryption is that the organization level, again for the very reasons that I mentioned, the numerous proxy and workflow roles that exist in healthcare where the individual is less important than the organization who has taken responsibility for the transaction.

To give an example for CommonWell we have an enrollment services wherein an organization enrolls a patient and is expected to provide to that patient meaningful choice to participate in the CommonWell linking service. The person who actually does the enrollment often is a registration clerk but the identity of that registration clerk is in many cases less important than the fact that this registration clerk has been dually authorized by the organization to play the role that they're playing.

With regard to patient identity CommonWell has found that the use of high assurance patient identifiers absolutely improves the linking and matching of patients across settings of care. We use existing high assurance identifiers such as state issued identifiers and it would be highly valuable if there was an ecosystem of higher assurance identifiers that could be offered.

We have the mechanism to identify the strength, we follow NIST-like levels of assurance. We would have the ability to use a higher level of assurance if such was available, we've currently reserved that for things like biometrics, but to the extent that there was a well-established ecosystem across the country of higher assurance identifiers that would greatly facilitate our ability to match and link patients.

Finally, we would recommend that those higher assurance identifiers be built on top of the existing identifiers that patients already know and use that might include state issued identifiers such as driver's licenses, it might also include a mobile phone that has the ability to provide higher levels of assurance.

So in conclusion, we find that organizational identity is most important for information exchange in the provider level and that the existence of an ecosystem of higher assurance identifiers would be highly useful for patient identity matching and linking. Thanks for your time.

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

Thanks so much Arien. I don't know if we have Lisa finally join us, I know she was trying to dial into the –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Yes, I'm here.

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

Great, Lisa –

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Can you hear me?

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

Yeah we can hear you, welcome, okay, Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

I apologize, I was ready to speak. Okay, well, thank you Walter and Dixie and the committee for giving me the opportunity to give HIMSS perspective today on the NSTIC Initiative. I lead a department at HIMSS that has a focus on infrastructure technology as well as privacy and security so as such we work with our members on the myriad of technology challenges they face such as patient data integrity, patient data matching and identity and attribute, and role-based access management as it pertains to patient identity provider and enterprise identity and IT access identity.

I've been participating in the NSTIC plenary and the IDESG Healthcare Committee for some time now. We heard Jeremy Grant and Dr. Tom Sullivan earlier provide us with a compelling call to action for the health sector describing the opportunity created by the NSTIC for the entire US eCommerce marketplace as well as the opportunity for the health sector.

I would describe that opportunity as the joy of nexus of the ability to establish trust with patients and their provider uses of EHRs and other technology with the ability and opportunity to solve some ongoing technical and administrative challenges such as identity proofing patients and accurately matching patients with their data in the environment of an active health information exchange.

HIMSS concurs with the NSTIC four guiding principles that the identity solutions would be privacy enhancing and voluntary secure and resilient interoperable and cost-effective and easy to use. In healthcare we understand that before the exchange of patient information can take place a trust relationship between exchanging entities must be established and then credentials must be securely exchanged.

The interoperability challenge here generally involves the exchange of credentials and data between two or more possibly competing organizations that might use different identity solutions that then use distinct trust models and/or arrangements.

The goal is to enable trust and exchange credentials across these disparate ecosystems while at the same time offering choice and flexibility to those being credentialed. At the recent HIMSS conference a panel discussion was held on the progress of a recent NSTIC pilot with an access to healthcare enterprise. The overall goal was to provide patient access to EHR data and provider access to their health system using strong identity proof credentials and multifactor authentication.

We heard from Michael Farnsworth this morning discussing the status of the technical implementation and lessons learned so far. Of note, from that panel description, at the HIMSS Conference, Dr. Marshall Ruffin, Chief Technology Officer of Inova Healthcare was able to discuss the business value from this implementation from three perspectives that of the patient where the solution is patient focused, user centric, convenient, reusable and provides that comfort factor for the patient that providers always strive to provide and the reduced burden on providers by providing a secure consistent process and credential reuse and the ability to leverage multiple credential types.

The benefits to his health system included consistent authentication mechanisms, reduced cost, increased security, ability to allow non-network provider access, reducing cost when servicing low volume access, decreased administrative and maintenance overhead and positive perception to patients and providers.

Finally, Dr. Ruffin listed requirements and benefits for the health ecosystem as a whole, a focus on stringent data privacy, promotion of a privacy lens and solutions development, streamlined enrollment through efficient identity proofing augmenting existing mechanisms, market adoptions of reusable interoperable solutions and enhanced patient experience.

As the IDESG transitions to a self-sustaining structure that will rely heavily on private sector support and participation and in order to facilitate more widespread participation by the health sector this month HIMSS will be launching the HIMSS Identity Management Taskforce. The goals of this taskforce are to serve as a multi-stakeholder industry liaison group to national level initiatives on identity such as the NSTIC initiative and at the same time to focus on development and tools of resources that will help HIMSS members on policy and technical challenges relating to identity.

With this taskforce HIMSS hopes not to create a separate effort but rather to facilitate the participation of multiple stakeholders including providers and vendors and the NSTIC Healthcare Committee and at the same time facilitating awareness and education to our members.

My hope for the Privacy and Security Workgroup of this Committee is that we continue to evaluate the ongoing efforts of the IDESG and the healthcare pilots and assist with the required work to facilitate interoperable solutions and the technical standards that are so essential for future success. Thank you for the opportunity to provide my perspective. Walter?

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

Thank you so much Lisa, thank you for that testimony. I think we're going to go next to Tim. Tim are you on the line?

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

Yes, I am and thank you Walter and thank you to the committee for the opportunity to provide testimony today. A key strength of Kaiser Permanente's integrated health system is its ability to connect with our members through digital channels. For example in any given month there will be 5.5 million sign-ons to our secure patient portal with 1.5 million secure e-mails exchanged between patients and providers. And patients will review online over 5 million lab test results. Fully one third of our patient portal access is now coming through mobile devices.

Kaiser Permanente members access all of their digital services through their channel of choice using one set of secure identity credentials and understand the benefits inherent in a unified identity system. From Kaiser Permanente's point-of-view NSTIC is a welcome initiative. That being said, adoption of NSTIC identities within the healthcare community is possible but would be complex.

The use cases for why a strong portable identity is needed within healthcare differ by role and point to at least some degree of difference in core standards by role for credentialed provisioning, credential maintenance, proxy extensions of a provisioned identity and metadata accompanying credentials for identity matching between disparate systems.

A key differentiator between medical and general commercial identities involves the concept of relative versus pinpoint identity. For many commercial uses of identity credentials it possible for people to self-provision in identity with minimal information and as long as the person can use their credentials to reliably authenticate against them the same identity can be used in multiple situations with low risk.

When a relative identity is used in a fraudulent manner in commercial situations the losses are more often than not monetary with systems building into their business model some margin for loss. While for individual consumers fraudulent use of such identity credentials can have broader impact to things such as credit scores. There are methods, albeit difficult, to largely remedy identified problems.

However, if an identity is used to inappropriately access pre-existing medical information the cost for both the patient and the provider organization can be substantial and non-recoverable. Once medical information is released into the wild you can't undo the damage and you must know exactly who is requesting a release of medical information and their legitimate relationship to the patient before doing so through any automated system.

Within the patient realm reasonable first steps for moving toward an NSTIC identity would be to establish gold standards and workloads for identity provisioning and the establishment of necessary metadata which could allow for identity federation between patient portals.

Ideally, for an NSTIC-type patient identity to be truly and consistently portable there would need to be a commitment by all participating organizations to the perpetual maintenance of identities which they establish or alternatively outsource all identity functions to a trusted third-party.

Rather than forming a complete NSTIC health identity ecosystem in the near term it may be more viable to use NSTIC health industry supported standards in a limited way to provision identities within a given system to agreed-upon standards such that a receiving system can initially accept a claim's identity as valid, in turn the receiving system would provision that same identity within a phone system and in so doing except responsibility for its maintenance. In effect, establishing protocols for provisioned identities to be daisy-chained with identity maintenance functions passing from organization to organization rather than being centrally and perpetually maintained by the initial issuing organization.

In terms of patient identity standards sensitivity to population characteristics is necessary. Security controls should be usability tested with those who actually use them including the elderly and people with limited education. Aligned with NSTIC principles, credentialing procedures and security control should not widen the current digital divide do to their complexity or cost.

In closing, the management of medical identity management credentials is not trivial in terms of both money and time. While identity management is not the core competence of healthcare organizations, out of necessity this competence has been developed with substantial changes to existing identity management system, standards and procedures should allow for a migration path from old to new.

With the advent of NSTIC a re-assessment of the role of healthcare organizations in provisioning and maintaining medical identity seems prudent. That being said, deep participation by the healthcare industry is highly recommended with NSTIC soliciting and including both individual healthcare organizations and health standards organizations such as HL7 and WEDI into NSTIC Committees and programs. Thank you.

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

Thank you Tim for that testimony. We're going to go to Kevin. Kevin are you online?

Kevin Isbell, MS – Senior Director, Health Information Exchange – Kaiser Permanente/Care Connectivity Consortium

I am, thank you Walter and thank you to the committee for my testimony. In addition to my role at

Kaiser Permanente I also play a role as a Project Manager for the Care Connectivity Consortium or also known as the CCC.

The CCC is a provider led collaborative founded in 2011 and it's made up of Geisinger Health System, Intermountain Healthcare, Kaiser Permanente, Mayo Clinic and also OCHIN, and really committed to the promotion of health information exchange through support of international standards and also innovation in certain HIE technologies with a specific focus on how do we address hurdles like patient identity, consent management in the HIE arena.

My remarks are follow ups to Dr. McKay's representing Kaiser Permanente but will be focused very much on exchange between providers and some of the identity hurdles that we have been facing over the last couple of years.

As not a surprise the accurate matching of patient identities across the healthcare ecosystem continues to be among the greatest challenges for information exchange, problems related to patient identity correlation and a disambiguation of persons with similar demographic traits poses a significant patient safety issue and also effects the ability to locate patient records for health information exchange between disparate electronic medical record systems.

According to a recent internal research conducted by the Care Connectivity Consortium where we really looked at exchanges across our organizations on a national level using commonly available demographic traits for identity matching including last name, first name, date of birth, gender and at least one physical address, patient matching success rates ranged between 40 and 60%. This means that approximately half the time when a query for clinical data was attempted, for treatment purposes, the identity of the patient could not be confirmed such that potentially critical patient information could not be made available to support the best possible clinical outcome.

In addition to the obvious patient safety concern this limited patient matching success rate is a key dissatisfier for those needing to collect dispersed patient medical information like providers, medical systems and also the patients themselves and degrades the overall perception at least of the value of health information exchange.

There are varied reasons for this poor patient matching success rate, some key contributors include the lack of standard required demographic traits for patient discovery, no consistent current use of unique patient identifiers and also just varied levels of sophistication in terms of the identity infrastructures themselves for the participating organizations.

In conclusion, Kaiser Permanente and the Care Connectivity Consortium believe that incremental improvements are possible to facilitate better matching of patient identities for health record exchange obtaining industry agreement about standard demographic traits for patient discovery and enhancing the integrity of data sources will improve overall success rates but only to a certain point, we can only go so far.

Initiatives such as NSTIC which provide for improvements, excuse me the possibility of a verified and portable patient identity would appear to support enhanced matching outcomes on a much broader scale in the healthcare ecosystem. So, we certainly support it, we look forward to looking at our understanding the technical and operational considerations around NSTIC as it continues to emerge. Thank you very much and I'll participate in the question and answer session.

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

Thank you, thanks Kevin. We're going to move, last but not least, to Mike. Mike, are you on the call?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Yes, can you hear me?

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

Yes.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Perfect, thank you. Thank you Dixie and Walter for inviting the Department of Veterans Affairs to participate in these discussions today. To begin VA is fully committed to supporting the goals of the NSTIC Program as a federal agency we do work closely with the Department of Commerce and GSA and other federal agencies.

Some history to frame our responses to the questions, in October of 2011 OMB directed agencies to accept externally issued credentials in accordance with government-wide requirements as a way to encourage industry adoption of NSTIC. NIST and GSA stood up to multitier Tiger Team to develop FCCX which you've heard about as a way to address these challenges. VA participates in the Tiger Team due to our significant government to citizen interaction.

Citizens, in our case veterans, will be able to use credentials they already have as part of their normal business with their – or online business. FCCX will link to the VA's web portal, which we call Access VA and will be the gateway for the veteran to access services.

I'd like to talk now directly to the questions. The first question is related to how actionable and adoptable the identities ecosystem should be or it would be. So I would say that VA has experiences in this key initiative include participation in the GSA eAuthentication Initiative in 2010, the recent total integration of our patient authentication system with that of DoD and veteran use of that credential, several years' experience in the operation of VA's commercial identity federation services with linkages both to the VA's premier patient PHR, which we call My HealtheVet, benefits, portals and our clinical NPI.

In 2013 VA conducted a successful pilot to use a third-party credential where the authorized user request ended up in VA's network to a trusted VA authentication federation infrastructure portal. The credentialed protocol meets NIST compliant standards, implements single factor remote network authentication, remote identity proofing, password authentication to include security questions and device authentication and verification.

Based on this experience we do firmly believe that NSTIC is both actionable and adoptable for advancing our core mission-critical needs in support of the nation's veterans. With respect to barriers, gaps or disconnects in terms of technology we see that trustworthy correlation, mentioned several times already, have different identities across the enterprise to be a major obstacle. This is being addressed by the FCCX Program.

The second area of concern is privacy. The US Army Medical Research and Materiel Command in the May 2013 Health Information Technology Privacy and Identity Management R&D Roadmap quoted "in the absence of good, secure, traceable identity management methods and systems, privacy of patient data cannot exist and yet few patient identity management systems have maintained the development of patient privacy features in parallel with the aggressive pace for interoperability."

This statement summarizes well the concern that too exclusive a focus on NSTIC's identity and correlation activity may ignore NSTIC's other important goals which include privacy, each technical development should be considered for its potential to improve or detract from privacy objectives.

The established principals of privacy by design including privacy as a test criterion and privacy enhancing technology should be the preferred design approach. In terms of operations there are challenges to interoperability.

VA as a federal agency must comply with a number of standards, laws, regulations and directives that establish a federal policy framework that has no commercial equivalent. Federal agencies compliance with these policies may in fact inhibit interoperability with the commercial sector.

With respect to question four, do we envision a healthcare ecosystem separate from the identity ecosystem? So the core premise of NSTIC is the use of an equivalent credential to access other systems of interest to citizens. That said, a separate and segmented healthcare ecosystem may provide an air gap that sequesters healthcare information in some sense from potential compromise of credentials originating from non-healthcare policy domains the type of domino effect that George Fletcher referred to in the single point of volunteer vulnerability Eve Maler spoke to.

Major disclosures and breaches of commercial customer databases are unfortunately all too a common occurrence. The impact of a commercial breach in one domain which propagates forward may not equate in terms of risk and remedial action with those within the healthcare domain.

For example, loss of dollars due to credential theft in banking maybe compensated financially without loss to the victim. Loss of privacy, integrity and trust on the other hand may not be so easily restored. Also the interaction of HIPAA security and privacy between healthcare and non-healthcare domains may be a concern.

The relative ease with which a patient identity can be resolved and linked to the person's identity in other domains is exactly why these core identity attributes are required to be removed when de-identifying patient information under HIPAA, which raises the question, are the identity and attributes providers and brokers such as FCCX governed by HIPAA when exchanging this information on behalf of covered entities. From this perspective we see advantages to a healthcare ecosystem separate from the identity ecosystems as a security and privacy enhancing mechanism. Thank you very much.

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

Thank you so much Mike for that testimony. And I think we heard a variety of perspectives really from healthcare organizations both NTP-like systems as well as sort of provider networks, of networks if you will. So, I think we're ready to turn to our Q&A. So, Michelle?

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

David McCallie has a question.

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

Yeah, thanks, it's a broad question and I'm probably not going to form it very well, but it occurred to me, as we've listened all day, all morning to the presentations, that in the intersection between identity provider systems and the healthcare space the key event that has to occur is what somebody called binding, I forgot who first used that term earlier today, but it struck me that the – that when someone walks into a healthcare setting and brings strong identity proofing with them, they still have to be bound to the identity that that healthcare system knows them as typically a medical record number or something like and that the IdP services aren't going to solve the binding problem because they don't know your medical record number and if you're a hospital and you know who the patient is from the medical point-of-view you don't know how to select them from the IdP's set of offerings of people who look like the patient you're interested in.

So, the critical event is this place where – at the moment in time where binding occurs. And I just wondered if any of you would care to comment on that perspective and say, you know, maybe we need standards to support easy binding to independent IdP, IDR systems. Does that make sense? Am I asking a dumb question?

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

No, this is Tim McKay and it makes perfect sense. There is a need for both as you said taking the claim's identity and making sure that we're matching correctly against internal credentials.

So, I can give you an example with how we establish a credential for a patient portal and we do close to 100% of our establishment of initial credentials remotely that is people are using a web App to create their identity and through that the first step is collecting information, demographic information that both should be known by the individual and then is also related to their identity within Kaiser Permanente so information that they could get off their medical card.

So, we use that as sort of a first step to check our internal systems to see if we can find an identity to potentially bind against and then use a second step of identity verification using knowledge-based authentication with presenting challenge questions we use LexisNexis as a vendor we constantly hone the set to make sure that the information can't be easily called from social media sources and then through that probably close to 80% of the folks who start the registration process can complete it by answering the questions correctly.

We also provide a task that if people either can't answer the questions or choose not to there is a bit of a creepy factor with KBA and we want to offer people the ability to have a secondary path. So, in that case we will send a one-time code to their address of record without exposing to the person what that address of record is and upon successful entry of that code they have credentials that can get to any piece of information within the system that we expose through the portal.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

So, David, this is Lisa Gallagher may I add to that?

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

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

So, this is exactly the type of work that we need to do in the health sector and I think the question goes beyond just, you know, standards for making that finding. I think there are also some policy questions in that binding process that bubble up that we could help facilitate a discussion on.

So, really what are acceptable ways in healthcare to do that binding and then, you know, sort of, you know, go from there as far as the policy aspects of it.

So, when it comes to the connection at NSTIC there is, you know, the framework and the principles and the work that's being done through the pilots but there is definitely some work that needs to be done in this sector, you know, by those who participate in the healthcare committee, our taskforce but also as the HIT Standards and Policy Committees as well.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

This is Mike David I'd like to make a comment if I may as well?

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

Please Mike.

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

Yes, go ahead, go ahead Mike.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Yeah, the topic of this binding is complicated by the fact that existing patient databases and MDI's were not put together using the, you know, NIST 800-63 and levels of assurance for the identities that are there. So, we're often trying to bind with fuzzier identities within the EHR where there – actually, a single patient had duplicate IDs or IDs may be shared among, same IDs may be shared among different patients.

So, there is a complex – we're not trying to bind, you know, one-to-one equal things. The one – it's a process, it's a long process to upgrade healthcare database to bring it up to the level of assurance that we would get from, you know, identity proofing somebody at some level of assurance for security purposes.

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

Yeah, this is David, I'll give you an anecdote of what led to my thinking about it this way and I've shared this story with our group before so some of you if you've heard this before, you know, please bear with me.

But one of the major KBA services has me confused with my father despite my attempts to correct it, it's persisted for years and I have actually learned how to answer their questions based on whether the question is about me or my father because I happen to know enough about my father to be able to answer the questions. And almost to a – without exception the relying parties who have invoked the KBA have been satisfied even when I complained to them verbally that this is not me you're validating against this is my knowledge of me aggregated with my father, they're perfectly happy to accept that.

And what that leads me to believe is me proving that I am who they want me to be is different from them actually knowing who I am and the binding would be a point where a patient physically standing there says "I'm going to use this strong identifier to identify myself in the future, please bind to it because I can prove at your portal that I am the guy who is standing here." The fact that outside in the IdP space that might or might not correspond to somebody with my name is somewhat irrelevant.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And this is Tim, I do understand that attack vector and it's something that we have looked at and tried to put some compensating controls in place. I do think your perspective of having some additional information that we could use for patient binding would be extremely helpful and very much welcomed.

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

Thanks.

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

Thanks, Michelle, do we have any more people in the queue?

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

We do, we have Peter Kaufman.

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

Thanks and I would very much like to thank all the presenters today it was a really interesting way to spend my day and I learned a lot. My question especially is addressed to Kevin.

It's sobering to hear how poor the matching is used in current data and fields and I understand the history, Tom Sullivan is cringing at this point, history of strong aversion to national patient identifiers but I'm disappointed that you and the others didn't even mention the topic even a voluntary identifier or an identifier with an opt in or an opt out because it would solve so many of these issues that we've created just to try to protect privacy that we're obviously, from the last comment, not protecting at all.

Kevin Isbell, MS – Senior Director, Health Information Exchange – Kaiser Permanente/Care Connectivity Consortium

Yeah, this is Kevin. I appreciate your comments. To be honest I did mention it, I contributed to one of the contributors I would say to our poor matching rates is the lack of unique identifiers. With that said, specifically to a universal ID I think there's been a lot of discussion today about why that's not in place and in essence I think the Care Connectivity Consortium and other groups that you've heard from are doing the best we can with what's readily available either on the eHealth exchange or otherwise in terms of exchanges that are going on across the country.

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy & Security – Healthcare Information & Management Systems Society

Well, Peter, this is Lisa Gallagher, if I may? I did not mention it but I would say that the ONC through their patient matching initiative has had a number of meetings with industry stakeholders on the topic of improving patient matching and significantly at the last meeting that they had the stakeholders present mentioned that they as industry representatives wanted to put the topic of a unique identifier back on the table while understanding the statutory prohibitions at the federal level that this was something that was still on their minds to discuss as a potential solution for this problem. So the dialogue is still ongoing but there are some challenges there.

Kevin Isbell, MS – Senior Director, Health Information Exchange – Kaiser Permanente/Care Connectivity Consortium

And if I may, this is Kevin one more time, just to add onto that comment, as an organization, Kaiser Permanente and also as a consortium, the CCC, we would be very interested in that discussion. We certainly see the value in a unique identifier and if there can be support in such a way that it's patient selected or elected we'd be very supportive of that and would like to participate in that discussion.

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

And so would just about every vendor out there.

Kevin Isbell, MS – Senior Director, Health Information Exchange – Kaiser Permanente/Care Connectivity Consortium

Sure.

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

This is David McCallie speaking on behalf of CommonWell since Arien had to leave, that is exactly what CommonWell provides as a service to the vendors who agree to join the quality alliance. The patient volunteers a strong identifier and then CommonWell – in other words they bind themselves – they provide a bindable identifier and the provider where the encounter is occurring binds that to the local medical record number and then CommonWell can match up that patient no matter where they go because they provide that same strong identifier at each of the encounter points. So, it's exactly the solution that Peter described.

The problem is that not everybody has a good strong identifier. Driver's licenses are suspect in some cases and they don't cover but a certain percentage of the population, they don't cover children and so forth.

So, Arien's point was we would welcome a broader array of strong identifiers for the patient to use as a voluntary national identifier for binding to the local records which would then allow the record locator to find them.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And this is Tim and I'd like to comment on that, that even when you have a strong identifier such as that, a driver's license number, it's rather subject to the same issues that were brought up in the earlier part of the Q&A.

If you have enough knowledge for example to answer the KBA questions correctly for an individual the odds are you have access to their physical wallet that you're in part of the family unit in such a way that you would have access to that as well.

So, while I'm not discounting that external identifiers can be used for binding, the use cases that surround it are fairly nuanced and I believe some consensus around the use of such external information for binding would be extremely helpful and a topic for NSTIC to address.

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

Yeah and this is David again, I think, you know, CommonWell would certainly appreciate if there was an external way to validate the identity, the match between the patient and the driver's license such as is being done in the Virginia pilot we would be very much interested in leveraging that capability if AAMV makes it available widely because I agree a driver's license in the hand is not completely good proof.

On the other hand, since this is voluntary consent by the patient to have their records linked and we're not using this identity for any other purpose such as billing, the people who want to commit fraud aren't going to volunteer to provide the identity in the first place.

So, we get pretty good results given that we have a narrowed use case somewhat along the lines of what I think Mike Davis was suggesting that we need a healthcare specific identity space because you don't really want to tangle it with these other business motives.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

So, this is Jeremy jumping in, you know, two things, one I think the concept of what you're talking about in terms of, you know, taking a strong credential and binding it to other attributes so that you actually have something that's usable in health systems – as we talked about the standards foundation one of the things that wasn't mentioned before is a technical committee that's been set up under OASIS focused on the concept of what's trust elevation which essentially looks at – if I'm starting with some sort of an identifier or credential that's at a low level of assurance how can I start to add other things to it and bind them all together so I can basically elevate up the levels of assurance.

It is focused around the NIST 4 levels, although this is being driven as, you know, it's an OASIS, you know, privately-driven technical committee but a lot of the foundations of it are really what is being done in the pilot involving Inova Health with the Motor Vehicle Administration. So, it's a – that also may be something that is worth taking a closer look at if this is really relative to a healthcare use case.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And this is Tim, I think there is something along that line of knowing how long a credential has been in use and is there any indication of improper use and that can also provide some additional level of assurance before allowing it to be federated more broadly.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Actually, I'll go a step further, just because it's been in use for five years does it still mean that it's good this week.

One of the things that is starting to come up within the issues that we're dealing with commercially is the questions of account fraud and account takeover and how you could set up a method of shared signaling between, you know, major identity providers in the ecosystems so that if an identifier, an account is being used in a fraudulent fashion how do you then get a signal out there similar to the way that, you know, your credit card can be revoked to revoke an account.

You know a classic example of that, you know, if I have a Gmail account that has been taken over and is suddenly being used to set up a number of fraudulent accounts, if there is a way to detect that how do I alert others who might be looking to use that Gmail account, you know, of the fact that this thing is no longer necessarily in control of the hand of the person who it was issued to or potentially even a person at all it could be a bot that's running it and look for ways to then handle revocation.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And speaking to that point, there is something about using any one control or any one data point for being able to perform binding is unwise. That there is something about creating algorithms that have collections of control that in combinations of one or many would be able to provide a higher level of assurance before binding to another entity.

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

Yeah and this is David, I was specifically talking about the use case of consumers and healthcare systems and in person binding which is not certainly the entire gamut of use cases but it's an important subset and that –

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

It seems to me that we could use some methods of identity proofing than is available in the current NIST specification, you know, in the VA, this is Mike speaking, we have a number of homeless veterans. They don't necessarily have homes or driver's licenses, they may have a cell phone, but – and we probably have biometric data on them their DNA and fingerprints and things like that but those are not usable.

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

Right, good point, that was the – yeah, we touched on that earlier.

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

Yeah, this is Walter, I wanted to jump in because my question or one of my questions I wanted to ask was about the role of biometrics on this identity proofing process and the binding that David was talking about.

But, Mike it sounds like you're saying that is not workable or it does not work? Could expand a little bit on that? And then maybe to others, what's the role and the current status really of the use biometrics with identity proofing that can be also linked to this entire ecosystem of identity management?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

I think it's a work in process. NIST 800-63 is fairly specific on how identity proofing is done biometrics is not included. I've talked to NIST about this and suggested, you know, that we might in a future edition, and you know that's a long process, provide other mechanisms to account for, you know, the business case that we have of, as I mentioned, veterans that don't have those kinds of credentials that they're looking for, for identity proofing. So, biometrics is certainly a good way to approach that, you know, something you are as opposed to necessarily having, you know, credentials like driver's licenses.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And this is Tim in the research that we've done biometrics are viable when you're looking at authentication authorization services within one set agency. The enrollment of a biometric is not trivial and then being able to use the biometric in a federated way becomes even more problematic.

You're needing, especially in remote situations to standardize on leaders, you're needing to standardize on algorithms, you're needing to deal with issues such as Apple is dealing with now with biometric laws where the biometric degrades over time. In many ways I think, especially in looking at a NIST-type identity biometrics seem premature.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Well, I'm speaking about, this is Mike again, veterans that have already had biometric information collected as part of their active duty service and have left and now –

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

Sure.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

So, this –

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And is perfect in working with the VA, but for them to use that as an identity, way of identity proofing for crossing over to another agency's HIT would pose way more of a problem, it's the portability of where I think we run into trouble.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

So, I'm not actually sure I agree with that, if I've been fingerprinted while I'm in military service and then the VA were to use, this is all hypothetical of course, and the VA were to then take advantage of those biometrics that were already in a database to verify that I'm the veteran who I claim to be why is it that I couldn't then use that at social security or IRS?

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And probably within –

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

One way to think of it –

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And probably within the government realm you could but when you're trying to use that as a more – a broad portable identity that would be more problematic.

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

Well, they'd all have to subscribe.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

This is Cathy Tilton, I would respectfully disagree with that I think there are methods to allow the use of the biometrics in a distributed environment.

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

But you – so this is David speaking again as CommonWell, we looked into this and the cost of deploying that biometric acquisition device that all the providers that would want to be able to participate was prohibitive. So, it may get cheap enough someday to have everybody have this, you know, a common set of standard, good quality biometric acquisition devices but we're not there yet.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

Well, it depends on which biometric modalities that you're interested in because for example voice and face you can use your mobile device today to do that.

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

Yeah, face isn't good enough and voice isn't reliable enough.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

This is – hello?

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

I mean, we've – those didn't meet our needs.

Cathy Tilton, MS – Vice President, Standards & Emerging Technology - Daon

I would suspect that you would want to use them as a second or third factor not as the primary factor.

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

Agreed, agreed.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

And it's argumentative I think whether biometrics are less reliable than weak passwords that we use today.

I have a biometric scanner on my little laptop which I love but on the other hand, the VA, as a federal agency, our employees all have smart cards and our identity proof is LoA 4 and we use PINs and our smart cards to log in, it's a wonderful system.

I wonder with all the money and effort and time we spend on this question why issuing smart cards to citizen's wouldn't be more cost-effective in the long run.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

I'm actually happy to tackle that one if you really want to, but I'll leave it to the committee in terms of what they want to get into.

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

Yeah, start with politics.

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

Yeah. Okay, let me, if I may ask just one other question, before that I guess I want to check with Michelle to see if there is someone else in the queue too or –

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

Yeah, so Walter you were in the queue with questions and then Leslie Kelly Hall has been waiting for a while as well.

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

All right Leslie, why don't you go ahead and then I'll ask after you?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thanks, Walter. This is following up on the question of the patient having a particular ID created and having the binding process that David described go on and I'm curious if in any of your pilots you included patient generated health data, went through this process, passed credentials that were at a high degree of trust so that an organization outside of your own would accept that information from a patient as coming from a source, the patient, with a very high degree of confidence that this person has been identity vetted and that your organizational level has actually stated yes, this is a patient and they are able to provide information to us and we are passing this on to you as trusted information while provenance included.

Because, today it seems the focus is on about how the provider uses an identity we all agree to and perhaps is bound to a medical record within an organization. But as the consumer gets more involved and is provided digital access to this ecosystem there will be the same expectations as in other industries of being able to pass information, share information and interact with other systems. So, I'd like to ask about your thoughts of natural evolution of the patient involved in this? Thank you.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

This is Jeremy, I can jump in, but let me actually ask our pilots who are still on, assuming they're still on, if they'd like to hit that one first?

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

Yeah, Jeremy this is Mike, and I'm glad you kind of teed that up because, you know, this is one of the things that we've been looking at and I think I referenced it in my presentation about use of patient data, demographic data and specifically for the purpose that you're talking about is using externals from a healthcare system.

So, a good example of that in one of our use cases is when you become a patient you provide a lot of information, your insurance information, your driver's license, your phone number, contact information and while the health care system that you provide it to can use it for purposes of providing services, is another healthcare system that either may be loosely, you know, associated with that healthcare system or not, able to leverage that demographic information that's being deemed authoritative if the patient consents for its usage.

And so you start getting into the questions about, well, you know, can we can release it, if we can how much do we release, how authoritative is it and then you get into the next part of the dialogue which is, well how was it collected, was it collected in a standardized fashion, you know, what is that standard for, you know, the collection of it and the storage of it, because if one healthcare system just allows you to pick up the phone number and call and change a phone number and doesn't really do a good job of identifying if that's indeed you, and then another healthcare system has relied on that as a method of authentication from an authoritative source now you've just broken the chain of trust.

And so, you know, there may be some opportunities to start looking at some of that standardization of how those attributes are collected and where they're stored and which ones are considered durable and which ones aren't.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Could I follow up with that?

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

And this is really – sorry, go ahead.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I think – just – what you've just described is a problem whether it is a provider going outside a network or getting an ID from an outside healthcare or a patient. And so, it's back to a person centric approach who might have tasks that demand a higher level of assurance and a higher level of trust than other tasks.

A view only for instance might have – it has certainly a lower level of a risk for one patient, one view than a service call that asks for a download of all patients with diabetes, which has a higher degree of risk and may still be used as necessary for care by a provider who is responsible for a particular population of sorts.

So, is there an opportunity to learn from all of this to apply to more of tasks that are inherently more or less risky versus people who are inherently professional, non-professional because a provider is at some point a patient, a patient also might be a provider and so forth. So, I'd love your comments. Thanks.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

So, I would jump in, this is Jeremy, and actually, you know, getting back to the question of whether this actually needs to be a health ecosystem or it can be, you know, part of a broader national ecosystem that, you know, a lot of what we're seeing in terms of trends, you know, really suggests the latter, but what enables those things are trust frameworks that actually, you know, basically include the rules that will show how a single, you know, solution can actually be used across multiple sectors.

You know, certainly while we talked about the, you know, AAMV pilot with Inova this is not an Inova pilot this is a pilot with the DMVs and its envisioned that after this credential, you know, is used to access something at Inova that a citizen in Virginia could also use it to access a state government website or perhaps another commercial party.

We have another pilot who didn't testify today, a company called ID.me that has a brand called Troop ID as part of what they are developing in the pilot they, you know, essentially will be developing a solution that will be seeking approval at LoA 3 under the GSA FICAM Program that Anil testified on earlier which would then enable a credential that could be used both to login in say to get a veteran discount at Overstock.com to also be used to login to access, you know, benefits or health information at the VA. Its trust frameworks that enable these sorts of sort of cross sector use cases.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And this is Tim, at Kaiser we have done some research looking at combining identities for different internal populations who use our services so looking at brokers and employers who have identity credentials who are also our patients and pretty much uniformly people do not want to cross over those domains. So if you're a broker and have access to say your book of business you want separate credentials for accessing the portal as a patient.

So, you know, hard to say, you know, how this might evolve over time but I think there is something there to understand the mental model of when people are using their identity credentials.

The second thing to consider is the metadata trail that would accompany any use of credentials and are there ways to be able to segment off of medical metadata, for lack of a better term, from that which is used for commercial purposes, because when the crossover happens there are way unexpected consequences like Target's disclosure of offering a young woman coupons for baby items and her father finding out that way that she was pregnant.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

So, here's a – two points on that actually, one on the fact that citizens want segmentation of their credentials I actually don't know that's the case, I think if they're given the choice, we've seen a lot of examples when they're given the choice to use a credential that they already have they do so.

Facebook Connect, is for better or for worse, say what you think about its security or privacy, but it's the single most successful federated identity application the world has ever seen.

When I was at HIMSS a few weeks ago the folks at Allscripts were demonstrating their App to download personal health records, they allow you to either a user name and password or login with Facebook or Google or several other, sort of, you know, what would be considered social identity providers and when we asked what people are actually doing with it they reported, that I think, about 80% of their users are actually leveraging Google or one of the other IdPs to access their health records, which then of course does raise some questions about things like metadata.

One of the benefits of the GSA FICAM Trust Framework Program that Anil talked about earlier is that a requirement to become certified is that the firms that are acting as IdPs specially pledge to only collect limited data and not actually, you know, tee something up where – the easiest example would be if I use Google to log into the IRS do I get an ad for TurboTax on the next screen. So, they're precluded from doing that.

And then FCCX as an identity hub actually goes – introduces an extra layer to further obfuscate how credentials are being used and what kinds of particular applications to actually create that kind of, really a technical dividing line that can enforce those policies.

Timothy McKay, PhD – Principal Solutions Consultant – Kaiser Permanente

And I do agree with that to a point. We're in the process at Kaiser of expanding the consumer identity space to include just not our current patients but former patients, people who are about to become our members, people who are non-covered subscribers, caregivers who are needing to – services on behalf of our members.

And the schema that we're looking at were the – things like Facebook Connect up to a point. So there is a point where when you're crossing over and going from things like accessing newsletters and general information to then moving into a realm where you're accessing direct patient information, especially on behalf of others, but the situation changes and the need to sort of upgrade the identity credentials becomes paramount.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

I would agree with that completely.

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

Michelle, I hate to interrupt and this is a great conversation, but we have gone over time here and so I'm – Michelle I think it's time for us to go onto the next, which are, what our closing remarks? Walter, did you want to say anything to close the final panel?

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

I had actually a quick question and I think it's an important one because it's really the one related to the standards, back to the standards and it was about – and this could be a very short one, this is about the experience or, you know, particularly CommonWell and CCC any experience – you know, we heard today a lot of different standards being used like OpenID Connect, OAuth and SAML and others, are you currently using any of these and what is your experience with those? And a very brief statement would be very appreciated.

Kevin Isbell, MS – Senior Director, Health Information Exchange – Kaiser Permanente/Care Connectivity Consortium

Walter, this is Kevin, I'll comment from the CCC's perspective, we are not using OpenID at this point or some of the other standards mentioned. We are utilizing SAML to a certain degree in relation to the eHealth Exchange. I think we've had good experience so far, certainly it's a standard that could be improved upon and certainly we have a lot of interest in some of these other standards that have been described today.

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

Thanks Kevin and David can you say anything about CommonWell?

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

Yeah, mostly we are using SAML because of our attempt to be consistent with the existing IHE profiles. I think there are few new services that we've built that use an OAuth derived approach but they are for sort of internal use.

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

Okay.

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

Yeah, this is Mike –

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

Go ahead, Mike?

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

Sorry, I apologize.

Michael Farnsworth, PMP, MCSD, OCP, SSGB – Vice President – Binary Structures Corporation

This is Mike from the CSDII pilot, we're actually using OAuth as our interface to Inova in order to access there and then we're also exploring the use of OpenID Connect and JWT for some of the attribute assertions. So, we're kind of moving in that direction, you know, kind of understanding where they're playing in the ecosystem.

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

Great and anybody else want to say anything about this? Mike Davis or...I know of course Mike you probably are using this.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

No, Walter, thank you.

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

Okay, all right, well, we thank you so much this I think has been a great way to conclude our hearing. I think the perspectives that healthcare providers bring into sort of the nuances and the applicability of NSTIC to healthcare has been very informative and so, I think we're going to – I'm going to turn it back to Dixie for her closing remarks and then we'll close out on the hearing, thank you.

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

Thank you very much Walter. I stated in my introductory remarks that the objective of this hearing was to provide the Privacy and Security Workgroup with an understanding of the current status of NSTIC, the maturity of the NSTIC-based standards and technology, and insights into the readiness of the standards and technology to be considered in our deliberations around potential national standards for identity and access management. And I think we certainly have met this objective.

I personally, have a much better understanding of NSTIC as a collaborative between the public and private sectors to achieve a capability for federated identity that extends both across the US, across agencies and throughout the world.

As for the NSTIC standards, I now know that NSTIC is not a set of new standards but is an effort to leverage existing standards that already are widely known and used and in fact these same standards are used in the new Blue Button Plus standard.

The experiences of the three pilots demonstrate the feasibility of implementing and using federated identity and also highlighted a number of important challenges.

As several people stressed the use of high assurance patient identifiers can improve the matching of patient records and so this is important with respect to patient safety and the overall quality of patient care and I really think it's important that we keep that perspective in mind. In fact, I think that's the most compelling argument for our pushing forward for high assurance identifiers and, as David mentioned, high assurance binding of those identifiers to patients.

The challenges that I heard today included the portability of identities between agencies and between healthcare organizations, the use of biometrics as part of identity proofing and potential HIPAA barriers were also mentioned by several of you.

Again, I want to thank all of our panelists for their thoughtful presentations and comments in response to our questions. I want to thank our Workgroup members for their thoughtful questions and participation and I also want to individually thank Walter, Julie Chua, Debbie Bucci and Michelle Consolazio for their help in organizing, preparing for and conducting this hearing. So, with that let's see, Walter did you want to add anything? Yes/no? You're on mute.

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

Yes, I was on mute, so sorry, thank you so much Dixie for those summary points. The only thing I wanted to add – I really thought that this was especially helpful in highlighting the importance of collaboration and participation and I think this served a lot more as a call for participation in these efforts from the providers and healthcare perspectives to be engaged and to be actively really participating in the direction that this is going to take us and so I think that was to me probably the single biggest message.

You summarized very well a lot of – some of the details of the findings in each of the sessions so I'm not going to repeat those.

And I also wanted to offer my thanks and appreciation to everyone who helped put this together. We really heard not just from the US but actually we had international participation as you realize and know and so I thank you again everybody for sharing your experiences and perspectives. So, back to you Dixie.

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

Michelle, I think it's time to open the lines for public comment.

Public Comment

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

I think so and thank you very much Dixie. Operator can you please open the lines?

Caitlin Collins – Project Coordinator – Altarum Institute

If you are listening via your computer speakers you may dial 1-877-705-6006 and press *1 to be placed in the comment queue. If you are on your phone and would like to make a public comment please press *1 at this time. We do not have a comment, Kathleen please proceed.

Kathleen Connor – Edmund Scientific

Hi, this is Kathleen Connor, I just had a simple question, I'm wondering about the HIPAA status of the ID providers and brokers who would be conveying the personal health information demographics that are typically excluded from release as – you know, if you're releasing de-identified information, so do they constitute business associates? Do covered entities need to establish business associate agreements with these folks? And that's my question thank you.

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

All right, thank you Kathleen, this is Michelle, this time is for comments but the committee does not have to respond at this time. Are there any more public comments?

Caitlin Collins – Project Coordinator – Altarum Institute

We have no further comment at this time.

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

Okay, well thank you very much to our participants and everyone who has worked so hard to put this hearing together we greatly appreciate all of your help.

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

Bye-bye.

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

Thank you.

Jeremy Grant, MS – Senior Executive Advisor, Identity Management – National Institute of Standards and Technology

Thank you appreciate it.

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

Thanks everybody.

W

Thank you.

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

Thank you bye-bye.

Public Comment Received

1. The Q&A following Panel 1 was excellent but I felt one area that was touched on by several of the panelist that didn't get enough exploration was in relation to the notion of the credit-card "liability-shift" model. and relying parties. We need to find out more about that!
2. Or your Iphone updates to a version that actually validates ephemeral Diffie Helmann TLS certificates and you find that someone has tried to spoof your messages and web browsing.

3. Covered entities that communicate directly with other covered entities without going through, or revealing PHI to a third party can be said to be using a Conduit under HIPAA and do not require any additional trust framework other than a verified identifier (say at LOA3) located in a Provider Directory.
4. In other words the concept that "trust" must be established first is false. And as Microsoft Research noted recently in PCAST big data hearings on patient privacy is that "trusted" systems that do not provide mathematical models for data privacy protection approach "an epsilon of infinity" leading to cartel formation. The reference is "Reflections on Trusting Trust by Ken Thompson, from the 1970s.
5. A valid LOA3 identifier from a patient with a valid digital signature and a unique patient id negotiated with a provider should be accepted for submission from a HIE of one.